wandera
a Jamf company

Rapport sur la sécurité du Cloud 2021

Voici une présentation approfondie des menaces qui pèsent sur les données de votre entreprise à travers vos ressources les plus critiques (vos terminaux, vos utilisateurs et vos outils d'accès à distance) ainsi que des conseils pratiques pour configurer vos outils professionnels et garantir une connectivité rapide et sûre à tous les utilisateurs en 2021.

EMEA 45 Mortimer Street
London W1W 8HJ
+44 (0) 203 301 2660

États-Unis 220 Sansome Street, Suite 1400
San Francisco CA 94104
+1 (415) 935 3095

Principales conclusions

- 52 % des organisations ont connu un incident lié à un logiciel malveillant sur un appareil distant en 2020, contre 37 % en 2019 – soit une augmentation de 41 %.
- Parmi les appareils compromis par des logiciels malveillants mobiles en 2020, 37 % ont continué à accéder aux e-mails d'entreprise après l'infection et 11 % ont continué à accéder au stockage Cloud.
- En 2020, 28 % des organisations utilisaient régulièrement un système d'exploitation présentant une vulnérabilité connue.
- Depuis la pandémie, nous avons constaté une augmentation notable, allant jusqu'à 100 %, des connexions à des contenus inappropriés pendant les heures de bureau.
- Les appareils Android étaient 5,3 fois plus susceptibles de contenir une application vulnérable que les appareils iOS.
- Les attaques de phishing étaient 6 % plus fréquentes le week-end qu'en semaine.
- En 2020, 4 % des utilisateurs se sont connectés à un point d'accès risqué, chaque semaine ; contre 7 % en 2019, toutefois :
- 15 % des organisations disposaient d'au moins un appareil utilisant une application qui a révélé des données de mot de passe, contre 11 % en 2019.

28 %

des organisations utilisaient régulièrement un système d'exploitation présentant une vulnérabilité de sécurité connue.

5,3 x

Les appareils Android étaient 5,3 fois plus susceptibles de contenir une application vulnérable que les appareils iOS.

Introduction

En 2020, de nombreuses organisations ont été contraintes de faire évoluer leurs pratiques commerciales vers un modèle entièrement à distance, tout en maintenant leur productivité. La politique informatique est donc révisée pour intégrer plus d'appareils, plus de réseaux et plus d'applications dans plus d'endroits que jamais.

L'entreprise sans frontières est là. Une enquête menée par Gartner auprès de directeurs financiers en mars 2020 a révélé que que 74 % d'entre eux ont l'intention de faire télétravailler certains employés de manière permanente.

Ainsi, les meilleures pratiques de sécurité doivent évoluer pour s'adapter à la nouvelle normalité. Les opérations informatiques les plus performantes se concentrent sur l'accès aux fonctionnalités des utilisateurs en dehors de leur bureau. Cela signifie que la stratégie de sécurité doit être plus flexible pour s'adapter aux différents besoins d'employés dispersés et faire du Cloud la priorité.

Les principaux experts du secteur pensent que le SASE (Secure Access Service Edge) sera le modèle d'architecture clé pour les entreprises innovantes qui s'éloignent des technologies traditionnelles. En effet, le SASE fait converger et aligner les fonctions de mise en réseau et de sécurité dans un service unifié natif du Cloud.

Si le SASE représente peut-être l'avenir, les entreprises doivent trouver les bons outils de travail dès aujourd'hui. Il est important de comprendre les cyberrisques et la façon dont ils peuvent être introduits dans l'organisation : c'est le but de ce rapport annuel.

Chaque année, nous analysons les menaces qui pèsent sur les appareils mobiles utilisés professionnellement. Notre portfolio de produits a évolué (pour intégrer des appareils autres que les smartphones et les tablettes), tout comme notre regard sur les ressources mobiles : il s'agit désormais également des employés, plus seulement des appareils mobiles.

Le rapport de cette année se penche sur les menaces et les tendances en matière de sécurité qui impactent les organisations dont les utilisateurs se connectent à distance – via une grande variété d'appareils et de plateformes portables – à une multitude d'applications hébergées dans des centres de données privés et publics.

FACTEUR DE RISQUE 1

Terminaux

Au cours des dernières décennies, l'introduction d'appareils portables a considérablement amélioré notre capacité à collaborer et à partager des informations, où que nous soyons. En 2020, la plupart des entreprises ont adopté le télétravail à temps plein, depuis le domicile de l'employé, en raison de la COVID-19.

Si la transition n'a pas été simple pour tous, elle l'a été pour certaines organisations, en particulier celles qui avaient déjà mis en place le télétravail à temps plein ou le travail à domicile occasionnel.

Dans de nombreux cas, les services informatiques ont dû prendre des décisions difficiles et rapides en termes d'autorisations d'accès aux données sensibles de l'entreprise. Ces décisions sont à l'origine d'incohérences majeures auxquelles certaines équipes informatiques et de sécurité n'étaient peut-être pas préparées.

Plus d'appareils et plus de types d'appareils

Au cours de la dernière décennie, les particuliers ont commencé à consommer de plus en plus de données Internet sur leurs smartphones. Il en va de même pour les données liées au travail, avec l'essor des applications SaaS mobiles, notamment les suites comme Microsoft Office 365 et les outils CRM comme Salesforce. Aujourd'hui, dans une entreprise type, 60 % des appareils utilisés pour le stockage ou la consultation de données d'entreprise sont mobiles.

Avant 2020, le travail mobile concernait essentiellement quelques employés en déplacement qui restaient connectés avec un smartphone appartenant à l'employé (BYOD) ou à l'organisation (COPE). Il concerne maintenant des personnes qui travaillent à temps plein depuis leur domicile, avec l'appareil qu'elles ont sous la main – et elles ont le choix. Cisco prévoit que le nombre d'appareils connectés aux réseaux IP sera plus de trois fois supérieur à la population mondiale d'ici 2023.

La différence entre « travailleurs mobiles » et « télétravailleurs à temps plein » commence à se creuser. Dans ce contexte, il devient de plus en plus évident que les outils de télétravail traditionnels ne sont pas suffisants pour de nombreux workflows, en tout cas de manière viable.

En l'absence de budget ou de chaîne d'approvisionnement permettant de fournir des appareils homologués aux utilisateurs, de nombreuses équipes informatiques permettent aux employés d'acheter et parfois même de choisir leur propre matériel informatique pour compléter leur poste de télétravail. Beaucoup optent pour des formats ultra-portables et convertibles dotés d'une énorme puissance de calcul, comme une Surface Pro, ou une tablette à grand écran faisant office de second moniteur, ou un MacBook Pro avec un ou deux moniteurs haute résolution. Les travailleurs qui avaient l'habitude d'utiliser des téléphones fixes acquièrent souvent un deuxième smartphone pour maintenir la séparation entre le travail et leur vie privée. La diversité des appareils est difficilement assimilable par les équipes informatiques.

Les travailleurs à distance utilisent également de nouveaux appareils portables offrant un partage de connexion sans fil, très utile pour accéder à Internet lorsque la bande passante Wi-Fi de leur domicile est saturée. Ils s'appuient sur les Verizon Jetpacks, les points d'accès mobiles et les Mi-Fis pour disposer de plusieurs options de réseau portable afin de maintenir des connexions Internet fiables à l'intérieur et à l'extérieur de la maison.

28 %

En 2020, 28 % des organisations ont fait les frais d'une vulnérabilité connue sur un système d'exploitation.

Version moyenne du système d'exploitation, modèles d'appareils et de systèmes d'exploitation

< Plus de 500 appareils		> de 500 appareils
11,3	versions différentes du système d'exploitation	39,4
1,4	Différents systèmes d'exploitation	1,6
1,8	Différents modèles d'appareils	2,6

En moyenne, les entreprises comptant moins de 500 appareils utilisent 11,3 versions du système d'exploitation différentes, sur 1,4 systèmes d'exploitation et 1,8 modèles d'appareils différents. En comparaison, les entreprises possédant plus de 500 appareils utilisent 39,4 versions différentes du système d'exploitation, sur 1,6 systèmes d'exploitation et 2,6 modèles d'appareils différents.

Le matériel utilisé pour travailler étant très divers, on assiste également à un élargissement de l'éventail de logiciels, qui ont toujours été particulièrement vulnérables. Beaucoup de nos clients prennent en charge une flotte d'appareils fonctionnant sous une combinaison d'Android, iOS, Mac et Windows 10. Ils essaient d'uniformiser une politique cohérente sur toutes ces plateformes, ce n'est pas facile lorsque chaque plateforme offre différents niveaux de contrôle et de fonctionnalité, ainsi que différents modes de distribution des correctifs de sécurité pour les systèmes d'exploitation vulnérables.

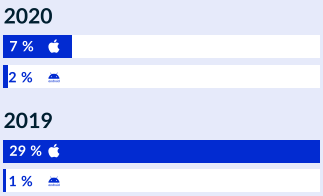
COUP DE PROJECTEUR SUR L'INDUSTRIE

En général, les appareils du secteur public sont moins menacés grâce à la mise en place de bonnes pratiques de sécurité. Cependant, ils utilisent souvent des systèmes d'exploitation obsolètes, puisque 4,4 fois plus d'utilisateurs utilisent des systèmes d'exploitation présentant des vulnérabilités de faible gravité, et 3,6 fois plus des systèmes d'exploitation présentant des vulnérabilités de grande gravité, par rapport aux moyennes mondiales.

L'absence de normalisation des appareils est la nouvelle norme

L'absence de normalisation des appareils pose de nouveaux défis aux équipes informatiques. Quand les entreprises n'avaient à se soucier que d'un seul type d'appareil, par exemple un ordinateur de bureau Windows, toute leur attention pouvait se concentrer sur un seul système d'exploitation. Il est possible qu'une partie de ces appareils étaient en retard de quelques versions, disons jusqu'à trois. Cela signifie que les équipes informatiques devaient connaître seulement quatre versions de systèmes d'exploitation pour en détecter les vulnérabilités. Aujourd'hui, les plateformes multiples étant la norme (Mac, Windows, iOS et Android), si l'on tient compte des versions obsolètes des systèmes d'exploitation, ce nombre est porté à 16. Conclusion : si vous donnez le choix aux employés, vous devez être prêt à prendre en charge de multiples appareils.

Version du système d'exploitation vulnérable



En 2020, 7 % des appareils iOS et 2 % des appareils Android utilisaient des versions vulnérables du système d'exploitation, contre 29 % et 1 %, respectivement, en 2019. Cette forte baisse des versions vulnérables d'iOS est probablement due à la série de vulnérabilités iOS très médiatisées qui ont émergé en 2019, affectant iMessage et FaceTime.

Le dilemme de sécurité des terminaux

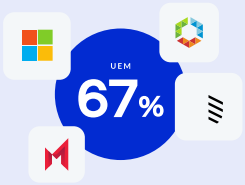
Les organisations aspirent à une forte sécurité des terminaux, mais elles se heurtent à des dilemmes communs : comment sécuriser temporairement les appareils des sous-traitants accédant à des données sensibles ? Ou : comment respecter la vie privée des employés sur des appareils BYOD tout en appliquant une certaine sécurité ? Les utilisateurs sont généralement opposés aux solutions de sécurité et de gestion. Ils ne veulent pas être espionnés et ils savent que ces solutions doivent assurer une surveillance pour détecter les mauvaises actions.

Nous savons que 70 % des failles réussies ont pour origine le terminal. Nous savons également que 83 % des entreprises déclarent qu'il est difficile, voire extrêmement difficile, de donner accès à des tiers (par exemple, des sous-traitants ou des partenaires de la chaîne d'approvisionnement). Il y a donc des améliorations à apporter en matière de sécurisation des terminaux non gérés.

Selon Verizon, 87 % des entreprises voient les menaces mobiles dépasser les autres types de menaces. Cela est probablement dû au fait que les appareils mobiles sont difficiles à gérer et à sécuriser, en raison de leur caractère personnel, et que les acteurs malveillants sont conscients de cette lacune en matière de sécurité.

Dans une étude, 92 % des entreprises du FT 500 ont déclaré qu'elles craignaient que l'augmentation de la mobilité de leurs employés ne représente un risque croissant de sécurité. Alors que la majorité des entreprises ont adopté des politiques BYOD (Bring your own device), la grande majorité (94 %) a déclaré que le BYOD a augmenté les risques de sécurité mobile.

Le télétravail va certainement perdurer, même lorsqu'une partie suffisante de la population aura été vaccinée contre la COVID-19. Les équipes informatiques doivent donc mettre en place des pratiques adaptées aux besoins d'un large éventail d'appareils et de réseaux gérés et non gérés. Elles doivent également s'assurer que les appareils distants ne restent plus en marge des opérations de sécurité en rassemblant les données sur les menaces de tous les terminaux dans le SOC.



Selon nos données, 67 % des appareils mobiles sont enregistrés dans un logiciel de gestion des appareils tel que MobileIron ou VMware Workspace ONE.

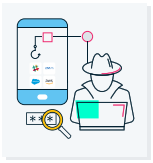
FACTEUR DE RISQUE 2

Utilisateurs

Les systèmes d'exploitation sont conçus pour atténuer la grande majorité des menaces de sécurité. Apple et Google ont pris de grandes mesures pour renforcer la sécurité de leurs systèmes d'exploitation et de leurs App Stores. Cependant, des risques peuvent être introduits par le comportement des utilisateurs. Pour les comprendre, nous devons examiner comment certaines attaques exploitent les faiblesses des utilisateurs. Mais nous devons également tenir compte des comportements qui affaiblissent la sécurité des appareils et ouvrent la voie aux attaques.

L'utilisateur est une victime ciblée

Les pirates contournent toujours les systèmes d'exploitation renforcés par des attaques d'ingénierie sociale telles que le phishing, qui vise à cibler et à tromper un utilisateur pour qu'il transmette des informations sensibles. Les utilisateurs peuvent également voir leur trafic intercepté par des acteurs malveillants qui exploitent le caractère non sécurisé du Wi-Fi public. En outre, les utilisateurs peuvent être victimes d'applications douteuses qui les exposent à des pertes de données, telles que des vols de données personnelles ou financières et autres escroqueries.



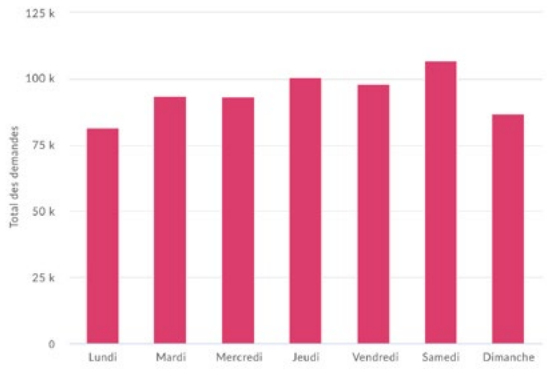
L'UTILISATEUR EST UNE VICTIME CIBLÉE

Phishing

Le phishing reste la première menace pour les utilisateurs d'appareils portables. Les attaques de phishing se concentrent généralement sur des sujets, des marques ou des thèmes qui ont de grandes chances d'attirer les victimes. Par exemple, chaque année, à l'approche de la période des impôts, on assiste à une recrudescence des attaques de phishing se faisant passer pour le Trésor public. De même, au cours du premier semestre de cette année, nous avons constaté une augmentation du trafic vers les sites de phishing liés à la COVID-19, et même l'émergence d'un faux site de vente de chloroquine en ligne.

Le graphique ci-dessous montre l'augmentation des attaques de phishing ciblant les travailleurs à distance au cours de l'année 2020.

En recherchant d'autres tendances de phishing qui ont émergé en 2020, nous avons remarqué que ces attaques atteignent le plus les utilisateurs le samedi. Les attaques par phishing sont 6 % plus fréquentes le week-end qu'en semaine. Cela renforce l'idée que, même si les employés ne sont pas en « mode travail », ils sont plus susceptibles d'être victimes de phishing sur les appareils de l'entreprise parce qu'ils sont moins sur le qui-vive.



L'UTILISATEUR EST UNE VICTIME CIBLÉE

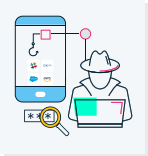
Attaques de l'homme du milieu sur le Wi-Fi

Le Wi-Fi présente un risque sérieux pour la vie privée en cas d'attaque de l'homme du milieu (HDM). Il existe deux types principaux d'attaques HDM affectant les utilisateurs mobiles. Le premier est celui où l'attaquant a le contrôle physique de l'infrastructure du réseau, par exemple un faux point d'accès Wi-Fi, et peut surveiller le trafic qui y transite. Le deuxième type est celui où l'attaquant manipule le protocole réseau censé assurer le chiffrement, exposant ainsi des données qui auraient dû être protégées. Il est alarmant de constater que plus de 80 % des employés utilisent le Wi-Fi public pour leurs tâches professionnelles, même lorsque cela est officiellement interdit.

> En 2020, 4 % des utilisateurs se sont connectés à un point d'accès risqué chaque semaine, contre 7 % en 2019.

Voyons comment l'impact des menaces Wi-Fi, notamment les attaques HDM, a évolué au cours de l'année 2020.

Lorsque nous avons réalisé cette étude, nous nous attendions à voir une baisse pour une raison évidente : les gens ne voyagent plus autant pour le travail qu'avant la COVID-19 (vers février-mars 2020). Sur ce graphique, nous observons une brève hausse en janvier, avec la reprise du travail, puis une forte baisse en février, avec l'augmentation du nombre de cas de COVID-19 : les entreprises ont commencé à annuler les voyages d'affaires et à conseiller aux employés de télétravailler pour assurer leur sécurité.



L'UTILISATEUR EST UNE VICTIME CIBLÉE

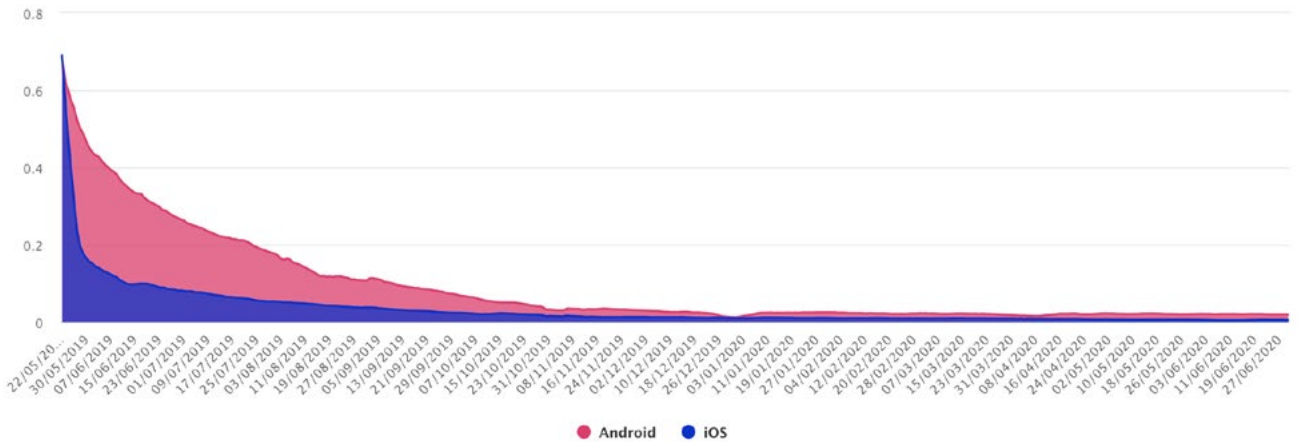
Risque lié aux applications

Les applications malveillantes, comme les logiciels malveillants, utilisent des techniques de plus en plus astucieuses pour échapper à la détection. Par exemple, les logiciels malveillants sophistiqués attendront un certain nombre d'étapes avant d'initier un comportement malveillant, qui affectera ainsi seulement un réseau spécifique, ou ils contiendront un code de commande et de contrôle dormant qui pourra être activé par un pirate à tout moment. Les contrôles de base, tels que ceux effectués par les App Stores, ne permettent pas de détecter les applications malveillantes sophistiquées, mais étonnamment courantes.

> En 2020, 52 % des organisations ont connu un incident lié à un logiciel malveillant sur un appareil distant, contre 37 % en 2019.

Outre les logiciels malveillants cachés dans les applications, les applications peuvent tout simplement être mal construites, sécurisées ou maintenues par les développeurs et donc sujettes à de dangereuses vulnérabilités, comme celles découvertes dans WhatsApp en 2019 et 2020.

> Les utilisateurs d'Android ont mis plus de temps à mettre à jour leurs applications après la découverte d'une vulnérabilité majeure dans une ancienne version de WhatsApp en mai 2019, comme le montre le graphique ci-dessous. De la mi-mai à la mi-juillet 2019, environ 85 % des appareils avec des versions vulnérables de Whatsapp avaient été mis à jour. En comparaison, seuls environ 50 % des appareils Android vulnérables ont été mis à jour pendant cette période.



Parfois, les applications contiennent une escroquerie ou une autre activité frauduleuse, et les développeurs introduisent souvent ces escroqueries par le biais d'une infrastructure publicitaire tierce. Nous avons vu des applications qui ont réussi à passer les contrôles officiels de l'App Store alors qu'elles étaient pleines de fenêtres publicitaires qui envahissaient l'écran de l'appareil et le rendaient inutilisable. Nous les appelons des applications potentiellement indésirables et 1 appareil sur 200 en a déjà installé une.

Certains développeurs peuvent même être assez négligents pour ne pas utiliser le chiffrement et exposer ainsi l'utilisateur (mais aussi son employeur) à un scénario de perte de données.

- En 2020, 15 % des organisations disposaient d'au moins un appareil utilisant une application qui a révélé des données de mot de passe, contre 11 % en 2019
- En 2020, les appareils iOS étaient 3,2 fois plus susceptibles d'être touchés par des fuites d'applications que les appareils Android.

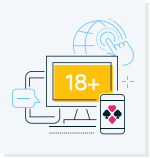
Notre analyse récente montre qu'une fois que le risque s'est introduit par une application non approuvée, il s'aggrave.

- avec au moins un appareil compromis par un logiciel malveillant sont 4,4 fois plus susceptibles d'être impactées par une fuite de mot de passe que les autres entreprises.
- avec une application vulnérable installée sur leur appareil sont 59 fois plus susceptibles d'avoir rencontré un trafic de cryptojacking que les autres utilisateurs.

Vérifier de manière indépendante la sécurité d'une application est une tâche laborieuse, mais nécessaire. Avec plus d'appareils que jamais, les utilisateurs ont accès à un monde d'applications. L'intention n'est pas toujours mauvaise. Un utilisateur peut vouloir utiliser un logiciel de fusion de fichiers PDF ou un autre outil de gestion de fichiers non approuvé par le service informatique, mais cette application peut comporter des risques. Le service informatique doit identifier les applications utilisées pour le travail pour deux raisons principales : (1) les risques qu'elles présentent doivent être vérifiés et (2) elles doivent être évaluées du point de vue de la productivité. Si elles s'avèrent sûres et bonnes pour la productivité, elles doivent alors être adoptées et protégées.

L'utilisateur prend de mauvaises décisions

Dans la section précédente, nous avons examiné le risque initié par l'utilisateur qui joue un rôle passif. Cette section examine les risques liés à l'utilisateur lorsqu'il joue un rôle plus actif, c'est-à-dire qu'il contourne délibérément les politiques de l'entreprise et les mesures de sécurité en place. Les utilisateurs peuvent s'attirer des ennuis en prenant des décisions irréfléchies, comme accéder à du contenu non conforme, ou en modifiant la sécurité de leur appareil : en le déverrouillant, en chargeant indépendamment des applications ou en désactivant les écrans de verrouillage.

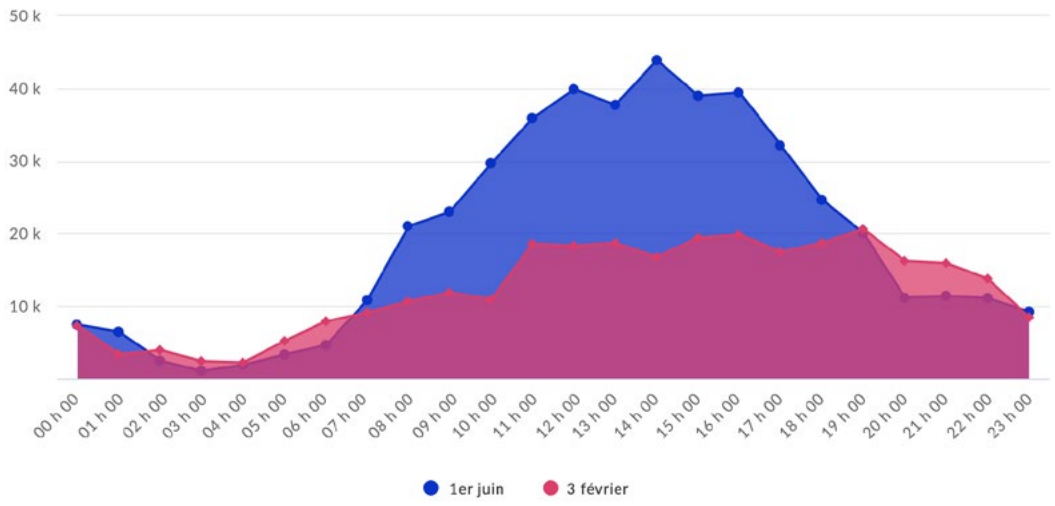


L'UTILISATEUR, MAUVAIS DÉCIDEUR

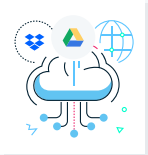
Contenu inapproprié

La présence dans votre infrastructure informatique d'appareils capables d'accéder aux coins les plus sombres d'Internet représente un risque pour votre entreprise. Lorsque nous parlons de contenus inappropriés, nous faisons référence aux contenus pour adultes, de jeux d'argent ou illégaux, qui sont beaucoup plus susceptibles de provoquer des fuites de données, d'utiliser des technologies non chiffrées et d'exposer les organisations à des risques. Il est surprenant de constater que de nombreuses personnes accèdent à la face cachée d'Internet en utilisant leurs appareils professionnels.

Depuis la pandémie, nous avons constaté une augmentation notable, allant jusqu'à 100 %, des connexions à des contenus inappropriés pendant les heures de bureau. Lorsque les employés travaillent à distance, il faut évidemment s'assurer que les politiques d'utilisation acceptable sont toujours respectées sur les appareils distants.



Le filtrage du contenu est un moyen efficace de faire appliquer la politique d'utilisation acceptable de l'entreprise sur toute une série de terminaux afin de limiter les risques de sécurité, de conformité et juridiques, tant pour les employés que pour leurs employeurs.



L'UTILISATEUR, MAUVAIS DÉCIDEUR

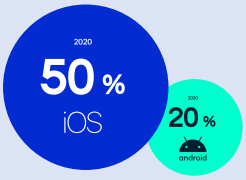
Contournement des mesures de sécurité

Les vulnérabilités ne tombent pas toujours sur les utilisateurs : parfois, ils rendent leurs appareils vulnérables, intentionnellement ou non.

Déverrouillage

Le déverrouillage et le débridage d'un appareil sont des configurations risquées qui permettent aux utilisateurs d'accéder au système d'exploitation d'un appareil et d'y installer des fonctions logicielles et des applications non autorisées. Ces tactiques sont également populaires parmi les utilisateurs qui tentent de contourner le verrouillage de l'opérateur sur leur appareil.

- En 2020, le nombre d'appareils iOS déverrouillés a augmenté de 50 %, et le nombre d'appareils Android débridés a augmenté de 20%.
- Les appareils déverrouillés sont 28 fois plus susceptibles d'être exposés à un trafic réseau malveillant que les appareils non déverrouillés.
- Les entreprises qui possèdent au moins un appareil déverrouillé dans leur flotte ont 31,6 fois plus de risques que les autres entreprises de voir leurs appareils exposés à un trafic réseau malveillant.
- Les appareils déverrouillés sont 33 fois plus susceptibles que les appareils non déverrouillés de contenir une application présentant une vulnérabilité connue.



En 2019, le nombre d'appareils iOS déverrouillés a augmenté de 50 %, et le nombre d'appareils Android débridés a augmenté de 20 %.

Chargement indépendant d'applications

Si certains utilisateurs d'iOS peuvent déverrouiller leur appareil mobile pour y installer des améliorations de sécurité, la plupart le font pour installer des applications non disponibles dans les App Stores officiels. Il est également possible d'installer des applications tierces sans que l'appareil soit déverrouillé ; il s'agit d'un processus appelé chargement indépendant d'applications. Il suffit à l'utilisateur de configurer son appareil pour qu'il fasse confiance à un développeur spécifique pour installer n'importe quelle application de ce développeur sans passer par l'App Store. C'est ainsi que de nombreuses entreprises installent des applications pour leurs employés sans publier ces applications sur l'App Store.

Google ne verrouille pas le système d'exploitation Android autant qu'Apple le fait avec iOS. Bien que la configuration par défaut d'Android n'autorise pas les applications chargées en latéral, il est possible de modifier les paramètres pour autoriser les applications provenant de sources tierces. Selon nos données, un utilisateur Android sur cinq a configuré son appareil pour autoriser l'installation d'applications tierces

Les utilisateurs qui chargent des applications indépendamment s'exposent à des risques accrus en matière de sécurité, car le processus d'examen des applications appliqué par Apple et Google dans leurs App Stores officiels est contourné et l'appareil est ainsi moins protégé contre les logiciels malveillants installés par inadvertance.

En 2020, 1 appareil Android sur 10 utilisé pour le travail contenait un App Store tiers installé (autre que Google Play).

COUP DE PROJECTEUR SUR L'INDUSTRIE - JURIDIQUE

Dans le secteur juridique, les utilisateurs sont 2,5 fois plus susceptibles de faire installer des applications en latéral sur leurs appareils que dans les autres secteurs.

COUP DE PROJECTEUR SUR L'INDUSTRIE - MANUFACTURE

Dans le secteur de l'industrie manufacturière, les appareils sont deux fois plus exposés aux logiciels malveillants que dans les autres secteurs. Cela peut être lié au fait que 50 % des utilisateurs ont installé des App Stores tiers et que les utilisateurs d'Android sont deux fois plus susceptibles d'avoir activé des sources inconnues.

Désactiver l'écran de verrouillage

Il est surprenant de constater que l'une des mesures de sécurité les plus simples disponibles sur un appareil mobile est encore souvent négligée : l'écran de verrouillage. Bien que la configuration de l'écran de verrouillage soit active par défaut sur la plupart des appareils, certains utilisateurs font tout leur possible pour la désactiver, laissant leurs appareils plus vulnérables en cas de vol physique. Cette pratique constitue également un indicateur d'une mauvaise hygiène de sécurité, et nos données montrent une augmentation de l'exposition à d'autres menaces des appareils sur lesquels cette mesure de sécurité de base a été supprimée.

- En 2020, 3 % des appareils utilisés pour le travail présentaient un écran de verrouillage désactivé, contre 6 % en 2019
- Les utilisateurs qui ont désactivé leur écran de verrouillage ont 16 fois plus de chances que les autres d'utiliser un système d'exploitation présentant une vulnérabilité connue
- Les utilisateurs dont l'écran de verrouillage est désactivé sont 2,4 fois plus susceptibles que les autres de voir leur adresse e-mail divulguée

COUP DE PROJECTEUR SUR L'INDUSTRIE - SERVICES INFORMATIQUES

Les utilisateurs au sein des services informatiques sont 2,2 fois plus susceptibles que la moyenne mondiale de désactiver l'écran de verrouillage de leurs appareils.

En 2020, 3 % des appareils utilisés pour le travail avaient un écran de verrouillage désactivé, contre 6 % en 2019.

FACTEUR DE RISQUE 3

Accès à distance

Nous avons examiné les risques liés aux appareils et aux systèmes d'exploitation, ainsi que les risques introduits par l'utilisateur, mais qu'en est-il des risques induits par ces appareils pour les applications professionnelles sensibles lorsque l'accès à distance est mal configuré ou n'est pas du tout sécurisé ? Quel type de protection devons-nous mettre en place entre l'appareil ou l'utilisateur à risque et les données sensibles des applications professionnelles ?

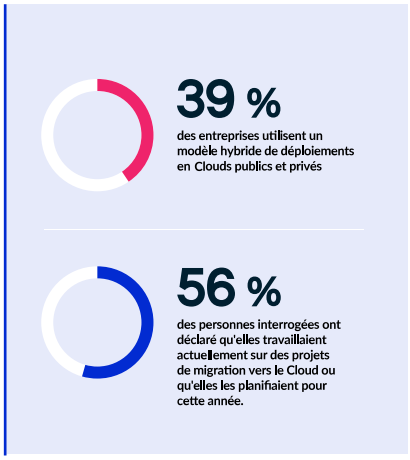
Lorsque nous parlons de la protection des applications d'entreprise, nous ne parlons pas de la protection des applications ou de la gestion des applications mobiles (MAM), nous parlons de l'accès sécurisé à la propriété intellectuelle sensible au sein de ces applications et des charges de travail exécutées dans le Cloud.

Selon le rapport 2020 de Cybersecurity Insiders sur la sécurité des télétravailleurs, 65 % des entreprises autorisent leurs employés à accéder aux applications gérées à partir d'appareils personnels non gérés.

En outre, selon le rapport d'IDC intitulé Remote Access and Security Challenges & Opportunities (Accès à distance et sécurité - Défis et opportunités), 40 % des cyber-failles ont en fait pour origine l'accès d'utilisateurs autorisés à des systèmes non autorisés.

Beaucoup d'applications professionnelles en beaucoup d'endroits

Les professionnels de l'informatique interrogés ont tous la tête dans le Cloud. Selon les données d'enquête du rapport O'Reilly's Cloud Adoption in 2020, 39 % des organisations utilisent une combinaison de déploiements de Cloud publics et privés dans un modèle hybride. En outre, dans cette enquête, plus de 56 % des personnes interrogées ont déclaré qu'elles travaillaient actuellement sur des projets de migration vers le Cloud ou qu'elles les planifiaient pour cette année.



Ces données nous indiquent que de nombreuses organisations ont adopté, ou sont en train d'adopter, un environnement décentralisé et hybride dans lequel les données résident dans diverses infrastructures. Certains garderont indéfiniment le contrôle de certaines applications, mais les solutions Cloud et SaaS ont permis de stocker les applications en dehors du périmètre de l'entreprise, faisant de leur accès un domaine critique pour les services de sécurité.

Les applications basées sur le Cloud sont appréciées sur de nombreux environnements de travail modernes car elles sont faciles et rentables à déployer, à gérer et à maintenir pour l'entreprise. Les services de Cloud publics et privés ont fait leurs preuves, ce qui les rend viables pour les entreprises de toutes tailles. De même, les solutions SaaS sont préférées pour certaines applications, car elles suppriment complètement les exigences de développement et la charge de maintenance pour l'organisation. Il ne fait aucun doute que le bénéfice l'emporte sur le risque lorsqu'il s'agit de SaaS : pourquoi creuser un puits quand on peut simplement ouvrir un robinet ? Gartner a prédit que les solutions SaaS généreront près de 105 milliards de dollars de revenus sur l'année 2020 uniquement.

De nombreuses entreprises déplacent certaines applications vers le Cloud et augmentent le nombre d'applications SaaS qu'elles utilisent, ce qui les amène à gérer un nombre inédit d'applications et d'emplacements. En outre, selon Okta, plus l'organisation est grande, plus elle utilise d'applications.

Le nombre d'applications logicielles déployées par les grandes entreprises de tous les secteurs d'activité dans le monde a augmenté de 68 % en quatre ans, pour atteindre une moyenne de 129 applications par entreprise fin 2018, selon une analyse d'Okta. Près de 10 % des entreprises disposaient de plus de 200 applications au moment de l'étude.

La nécessité d'un accès à distance moderne

Les entreprises avaient l'habitude de protéger uniquement le centre de données qu'elles contrôlaient physiquement. Les anciens outils d'accès à distance, tels que le VPN et le RDI, ont été conçus sur la base d'un périmètre d'entreprise et fonctionnaient correctement lorsque les applications étaient exécutées depuis le centre de données. Avec un modèle de sécurité de type « castle-and-moat », le système fait confiance par défaut aux connexions à l'intérieur du réseau. Cela signifie que des attaquants potentiels pourraient avoir accès à des segments entiers du réseau parce que les VPN et les RDI font implicitement « confiance » aux connexions, sans méthode solide pour vérifier l'identité de l'utilisateur ou contrôler la sécurité de l'appareil.

Selon l'IDC, le VPN a été utilisé dans 68 % des incidents majeurs impliquant des outils d'accès à distance. De plus, 40 % des cyber-failles ont en fait pour origine l'accès d'utilisateurs autorisés à des systèmes non autorisés.

Pourquoi l'évaluation continue des risques est-elle un élément important de la stratégie d'accès à distance ? Les chiffres parlent d'eux même.

- Parmi les appareils exécutant un système d'exploitation vulnérable en 2020, 1 sur 83 accédait à ses e-mails et 1 sur 6 accédait au stockage dans le Cloud au moment de la vulnérabilité.
- Parmi les appareils compromis par des logiciels malveillants mobiles en 2020, 37 % ont continué à accéder aux e-mails d'entreprise après avoir été compromis et 11 % ont continué à accéder au stockage dans le Cloud.
- Dans 42 % des entreprises dont les appareils sont compromis par des logiciels malveillants, au moins un de ces appareils accède aux outils de productivité.
- 1 appareil sur 200 accédant au stockage dans le Cloud a son écran de verrouillage désactivé.
- Dans 40 % des entreprises dont les utilisateurs utilisent des systèmes d'exploitation vulnérables, au moins un de ces appareils vulnérables accède au stockage dans le Cloud.
- 1,3 % des clients ont un appareil compromis par un logiciel malveillant en utilisant des outils de productivité, notamment Office 365 et Google Workspace.
- Nous savons donc que l'authentification de l'utilisateur ne suffit pas à protéger les données commerciales sensibles contre les appareils compromis. Quelle est la solution ? Les fonctions d'accès réseau Zero Trust constituent un changement fondamental par rapport à l'approche traditionnelle. Plus besoin de boîtes, d'appareils, ni d'appareils physiques. Et plus important encore : la sécurité réseau fournie par le Cloud est évolutive. Sans cela, vous ne pouvez tout simplement pas acheter suffisamment d'appareils pour protéger toutes ces données qui sortent du périmètre de l'entreprise et se retrouvent dans le Cloud.

En outre, les fonctions d'accès réseau Zero Trust peuvent effectuer des évaluations continues des risques des appareils qui demandent l'accès à vos applications sensibles pour s'assurer que l'appareil est conforme, ce qui peut signifier un certain nombre de choses : que l'appareil est sur un bon réseau, à l'endroit prévu, sans infections ni vulnérabilités et que l'utilisateur est autorisé à faire sa demande donnée.

42 %

des entreprises dont les appareils sont compromis par des logiciels malveillants comptent au moins un appareil avec accès aux outils de productivité.

Parmi les appareils exécutant un système d'exploitation vulnérable en 2020, 1 sur 83 accédait à ses e-mails et 1 sur 6 accédait au stockage dans le Cloud au moment de la vulnérabilité.

Recommandations

Même si l'on tente depuis des dizaines d'années maintenant de définir des normes informatiques d'entreprise, de nombreuses entreprises en sont arrivées à un stade où l'absence de normalisation est devenu la norme. Quels systèmes d'exploitation votre entreprise utilise-t-elle ? Tous. Quel type d'utilisateurs autorisez-vous à accéder à vos applications ? Tous. De quels endroits les utilisateurs sont-ils autorisés à travailler ? Partout.

Les solutions d'accès à distance sécurisé doivent être suffisamment souples et agiles pour permettre, et non empêcher, la productivité. Nous vous recommandons d'utiliser cette liste pour élaborer une stratégie de sécurité SASE moderne et adaptée aux besoins des environnements informatiques actuels.

Définissez les exigences en fonction des nouveaux cas d'utilisation impliqués par le télétravail

- Que souhaitez-vous permettre aux employés de faire sur leurs appareils : accéder aux e-mails ou aux bases de données sensibles ? Segmentez les données pour permettre un accès granulaire.
- Évaluez vos cas d'utilisation et définissez les besoins des employés en télétravail.
- Les exigences ci-dessus détermineront votre modèle de propriété des appareils : quels types d'appareils prendrez-vous en charge, qui en sera le propriétaire et comment seront-ils gérés ?

Connectivité

- En ce qui concerne la connectivité et les applications Cloud, déterminez ce que vous devez savoir sur les utilisateurs, les appareils, les réseaux et les applications avant de leur accorder l'accès aux ressources de l'entreprise.
- Limitez les utilisateurs aux seuls outils professionnels dont ils ont besoin, afin d'éviter que des comptes trop privilégiés soient exploités pour attaquer un grand nombre de systèmes.

Définissez un usage acceptable

- Passez en revue vos politiques d'utilisation acceptable existantes et assurez-vous que tous les types de terminaux sont pris en compte.
- Mettez en œuvre une politique d'utilisation acceptable pour chaque sous-ensemble d'appareils afin de contrôler l'informatique fantôme et toute utilisation non désirée, mais aussi de garantir la conformité réglementaire.

Élargissez les politiques de gestion des accès pour y intégrer l'état de risque des appareils

- Mettez en œuvre une solution GIA (gestion des identités et des accès) conviviale pour l'authentification aux applications d'entreprise sur tous les appareils, y compris les mobiles.
- Intégrez des évaluations des risques liés aux appareils dans vos politiques GIA pour tenir compte de l'exposition au risque des appareils.
- Assurez-vous que la posture de risque est évaluée en permanence pendant toute la durée d'une session.

Déployez une protection des terminaux sur tous les appareils. Une solution de sécurité basée sur le Cloud est particulièrement importante pour se protéger contre le large éventail de cybermenaces et de risques d'utilisation

- Assurez-vous que votre solution de sécurité dispose d'une forte capacité de détection des terminaux et d'une architecture intra-réseau pour empêcher les attaques avant qu'elles ne touchent un appareil.
- Assurez-vous que votre solution de sécurité peut traiter à la fois les cybermenaces externes (comme le phishing, les attaques de type « homme du milieu » ou les logiciels malveillants) et les risques liés au comportement des utilisateurs (applications chargées indépendamment, etc.)
- Pour tous les outils de sécurité, vérifiez que les configurations sont appropriées pour traiter les vecteurs de menace spécifiques à votre entreprise, tout en respectant la vie privée de vos utilisateurs finaux.
- Évaluez la capacité d'apprentissage machine de la solution de sécurité pour comprendre comment le moteur de menaces identifie et prévient les nouvelles menaces.

Déployez un UEM pour le contrôle des appareils

- Le cas échéant, déployez une solution UEM qui vous permettra de doter les appareils des ressources de l'entreprise et de procéder à des contrôles permanents de la conformité des appareils.

Revisitez souvent cette liste et réfléchissez aux changements à apporter en fonction des éléments suivants :

- Changements dans la taille et la composition de l'entreprise, par exemple en cas de fusions ou d'acquisitions
- Nouvelles réglementations affectant la manière dont vous traitez les données
- Évolution de la stratégie informatique
- Menaces constatées pour les employés
- Nouvelles applications dont les employés ont besoin pour leur travail