citrix chrome OS

Relever les défis de sécurité du travail hybride

Comment les solutions Citrix DaaS et Chrome OS aident les entreprises à mettre en œuvre des solutions de sécurité multicouches

Le travail hybride exige une nouvelle approche proactive de la sécurité

La nature du travail a considérablement changé au cours des deux dernières années. Les entreprises ont rapidement adopté des modèles de travail hybride, proposant à leurs employés une plus grande liberté quant au lieu, à la manière et au moment où le travail est effectué.

Au fil du temps, l'IT a mis en œuvre de nombreuses solutions ponctuelles pour rendre possible le télétravail, ce qui, dans certains cas, a entraîné un relâchement des contrôles de sécurité. Les cybercriminels étaient prêts à tirer parti de ces faiblesses et ont lancé une volée d'attaques. Le hameçonnage, les attaques par rançonlogiciel et les menaces sur la chaîne d'approvisionnement ont fait rage en 2020, mettant les stratégies, la propriété intellectuelle et la continuité d'activité des entreprises en danger.

Depuis lors, les équipes IT des entreprises ont réalisé qu'elles avaient besoin d'un moyen complet, intégré et homogène de maintenir la productivité des employés tout en sécurisant les données, les actifs et les réseaux essentiels. Et aujourd'hui, plus que jamais, elles considèrent Citrix Desktops as a Service (DaaS) et les appareils Chrome OS comme la solution combinée permettant de répondre à l'évolution de ces besoins.

Aujourd'hui, l'IT et la sécurité ont besoin d'un moyen complet, intégré et homogène de maintenir la productivité des employés tout en sécurisant les données, les actifs et les réseaux essentiels.

Les solutions Citrix DaaS sur les appareils Chrome OS offrent une meilleure façon de sécuriser l'avenir du travail. Cette solution conjointe propose une sécurité multicouche intégrée et des actions automatisées pour prévenir les violations. Citrix DaaS et Chrome OS fournissent aux entreprises la solution de télétravail la plus complète, sécurisée et rentable disponible aujourd'hui sur le marché.

Les menaces pour la sécurité se multiplient à l'ère du travail hybride

61% des entreprises ont eu du mal à faire évoluer la sécurité pour prendre en charge le télétravail.[1]

En 2021, les coûts mondiaux de réparation des cyberviolations devraient dépasser

6 000 milliards de dollars.[2]

L’IT doit faire évoluer la sécurité du travail hybride

L’empressement à prendre en charge le télétravail a introduit de nouvelles lacunes dans les architectures de sécurité que les équipes IT doivent désormais combler par une approche à long terme. Voici quelques considérations clés à prendre en compte pour votre stratégie de travail hybride :

Réduire la dépendance aux VPN

Les VPN d’accès distant ne sont pas les dispositifs de sécurité que beaucoup pensent qu’ils sont. Les VPN peuvent être connectés à des routeurs Wi-Fi domestiques non sécurisés, avoir un chiffrement mal configuré ou ne pas utiliser l’authentification multifacteur. Les équipes de sécurité doivent utiliser des solutions DaaS pour fournir un accès chiffré sans VPN aux applications, données et ressources qui sont exécutées dans le cloud, réduisant ainsi considérablement le niveau de menace.

Adopter une sécurité Zero Trust

Les solutions de sécurité traditionnelles, comme les VPN, ont été conçues sur le principe de « faire implicitement confiance » à quelque chose de connu. Mais les attaques modernes tirent parti d’identifiants de connexion compromis, d’appareils volés et de la possibilité d’insérer du contenu malveillant.

L’approche Zero Trust va à l’encontre du principe de confiance implicite et s’appuie sur le principe **« Ne jamais faire confiance, toujours vérifier »**, en supposant que tous les utilisateurs, appareils et URL sont suspects, sauf preuve du contraire. Les solutions de sécurité Zero Trust authentifient en permanence les utilisateurs, de la demande d’accès initiale à la fin de la session.

Réduire les risques liés à l’appareil

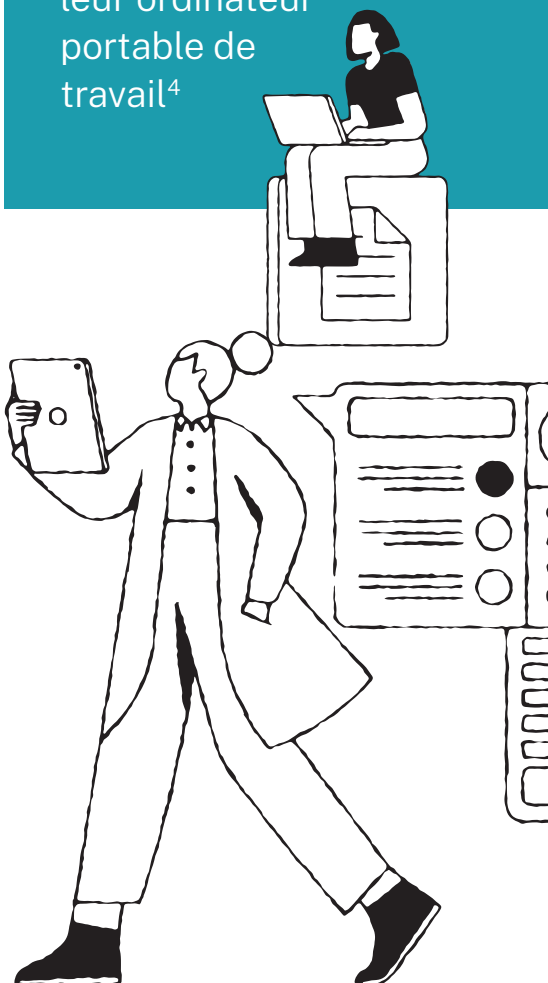
Travailler depuis des lieux publics augmente le risque qu’un appareil soit perdu ou volé. Sachant qu’un **ordinateur portable a une chance sur dix d’être volé et seulement 2 % d’être retrouvé,** la meilleure approche consiste à conserver toutes les données en dehors des appareils et à les stocker dans le cloud.[3]

Cette approche limite également l’impact d’un logiciel malveillant ou d’un rançonlogiciel car l’IT peut, à distance, désactiver un appareil compromis et effacer son contenu. Les profils, données, applications et postes de travail des utilisateurs restent sécurisés et disponibles dans le cloud.

Rationaliser la gestion de l’IT

L’utilisation de multiples solutions autonomes et processus manuels pour gérer les points de terminaison n’est pas adaptée. L’IT a besoin d’une solution de sécurité et de gestion holistique et intégrée qui diffuse de manière centralisée les dernières mises à jour de sécurité des applications et des systèmes d’exploitation depuis le cloud. Cette approche intégrée et centralisée permet à l’IT d’économiser beaucoup de temps et de ressources. Elle améliore également la posture de sécurité d’une entreprise en réduisant le nombre de solutions que l’IT doit gérer en permanence.

30 % des télétravailleurs laissent une autre personne utiliser leur ordinateur portable de travail[4]



Les solutions Citrix DaaS et Chrome OS répondent aux exigences du travail hybride

Citrix et Google s'associent depuis plus de dix ans pour permettre aux entreprises du monde entier de façonner l'avenir du travail hybride. **Les solutions Citrix DaaS sur Chrome OS fournissent aux entreprises une solution de télétravail sécurisée qui offre aux employés un accès en un clic à tout type d'application ou de poste de travail.** Les administrateurs IT bénéficient de cette solution intégrée, axée sur le cloud, avec des stratégies de sécurité granulaires et des fonctionnalités de gestion centralisée. Avec une sécurité intégrée multicouche et des actions automatisées, la solution combinée Citrix DaaS et Chrome OS aide les entreprises à activer, sécuriser et mettre à l'échelle le télétravail pour les équipes hybrides à l'échelle mondiale.

Les solutions Citrix DaaS sur les appareils Chrome OS sont :

Sécurisées
Les données sont stockées dans le cloud, les connexions sont chiffrées et les logiciels et systèmes d'exploitation sont mis à jour.

Intégrées
Les employés ont accès aux postes de travail virtuels et aux applications Windows, Linux, web et SaaS.

Simplifiées
Les solutions Citrix DaaS sur Chrome OS sont plus rapides à déployer, plus faciles à gérer et réduisent les coûts et les besoins globaux en maintenance IT.

Améliorer la sécurité du travail hybride avec Citrix DaaS et Chrome OS

Les solutions DaaS Citrix et Chrome OS répondent aux impératifs de sécurité des entreprises aujourd'hui et respectent les bonnes pratiques du secteur pour sécuriser le travail hybride.

Utiliser des appareils et des services sécurisés de manière native

Chrome OS et Citrix DaaS ont été conçus dès le départ en tenant compte de la sécurité. Comme toutes les applications et données sont mises à disposition depuis le cloud, sans aucun stockage sur l'appareil, la solution combinée est parfaitement adaptée au télétravail.

Citrix DaaS permet aux ressources d'applications et de postes de travail d'être hébergées sur des clouds publics ou privés et peut être configuré pour sécuriser en permanence toutes les connexions aux applications et aux postes de travail grâce à des stratégies de sécurité Zero Trust et un chiffrement TLS (Transport Layer Security). De plus, Citrix DaaS et Chrome OS proposent automatiquement des correctifs et des mises à jour de sécurité dans le cloud afin que l'espace de travail de chaque employé soit toujours à jour.

Permettre des modèles de sécurité Zero Trust

Face à l'augmentation des risques liés aux terminaux, les entreprises ont besoin d'une approche différente de la sécurité, qui adopte le principe « ne jamais faire confiance, toujours vérifier » pour toutes les demandes d'accès. Ce faisant, elles supposent que les tentatives d'accès sont malveillantes jusqu'à preuve du contraire.

Les solutions DaaS Citrix et les appareils Chrome OS permettent d'obtenir des modèles Zero Trust en mettant à disposition la sécurité au niveau des applications, tout en vérifiant en permanence l'identité des utilisateurs. L'IT peut utiliser Citrix Secure privé pour mettre en place des stratégies fines qui fournissent un accès contextuel aux ressources Citrix DaaS. Cela signifie que l'identité, l'appareil, l'emplacement, l'heure et le comportement de l'utilisateur ainsi que d'autres facteurs clés sont pris en compte pour s'assurer que l'identité de l'utilisateur et les sessions sont légitimes.

Google BeyondCorp Enterprise propose un accès sécurisé aux applications web en déplaçant les contrôles d'accès vers l'utilisateur et l'appareil. Si les appareils et les identifiants de connexion de l'utilisateur ne sont pas vérifiés, les demandes d'accès sont refusées. **Citrix Secure Internet Access** fournit une autre couche de sécurité basée dans le cloud qui protège tous les utilisateurs, quel que soit leur emplacement, contre les menaces les plus récentes.

Fournir des privilèges d'accès granulaires

Les solutions Citrix DaaS donnent aux administrateurs un contrôle granulaire sur les utilisateurs en appliquant des stratégies à différents niveaux du réseau, du niveau local à celui de l'unité organisationnelle. En contrôlant ces stratégies, l'IT détermine si un utilisateur, un appareil ou des groupes d'utilisateurs et d'appareils peuvent se connecter, imprimer, copier/coller ou mapper des disques locaux. Ces contrôles granulaires limitent les problèmes de sécurité, par exemple avec des travailleurs d'urgence tiers. De plus, Chrome Enterprise permet à l'IT d'appliquer plus de 500 stratégies d'appareils pour une sécurité et un contrôle de bout en bout.

Aucune attaque de rançonlogiciel n'a été signalée sur des appareils Chrome OS, qu'ils soient utilisés par des entreprises ou des particuliers.[5]

Comment Citrix DaaS et Chrome OS simplifient la gestion de l'IT

L'IT souhaite offrir une expérience utilisateur exceptionnelle tout en rationalisant les processus de gestion. Citrix DaaS fournit des processus plus simples et scalables qui proposent des avantages continus aux équipes IT, à mesure qu'elles gèrent la croissance accrue de l'entreprise.

Centraliser la gestion de l'IT

Citrix DaaS et Chrome OS fournissent une gestion intégrée et centralisée des appareils, des utilisateurs, des applications et des postes de travail depuis le cloud. Les administrateurs IT peuvent donc effectuer des mises à jour de sécurité de manière fluide et à distance, automatiquement en arrière-plan, pendant que les employés continuent à travailler.

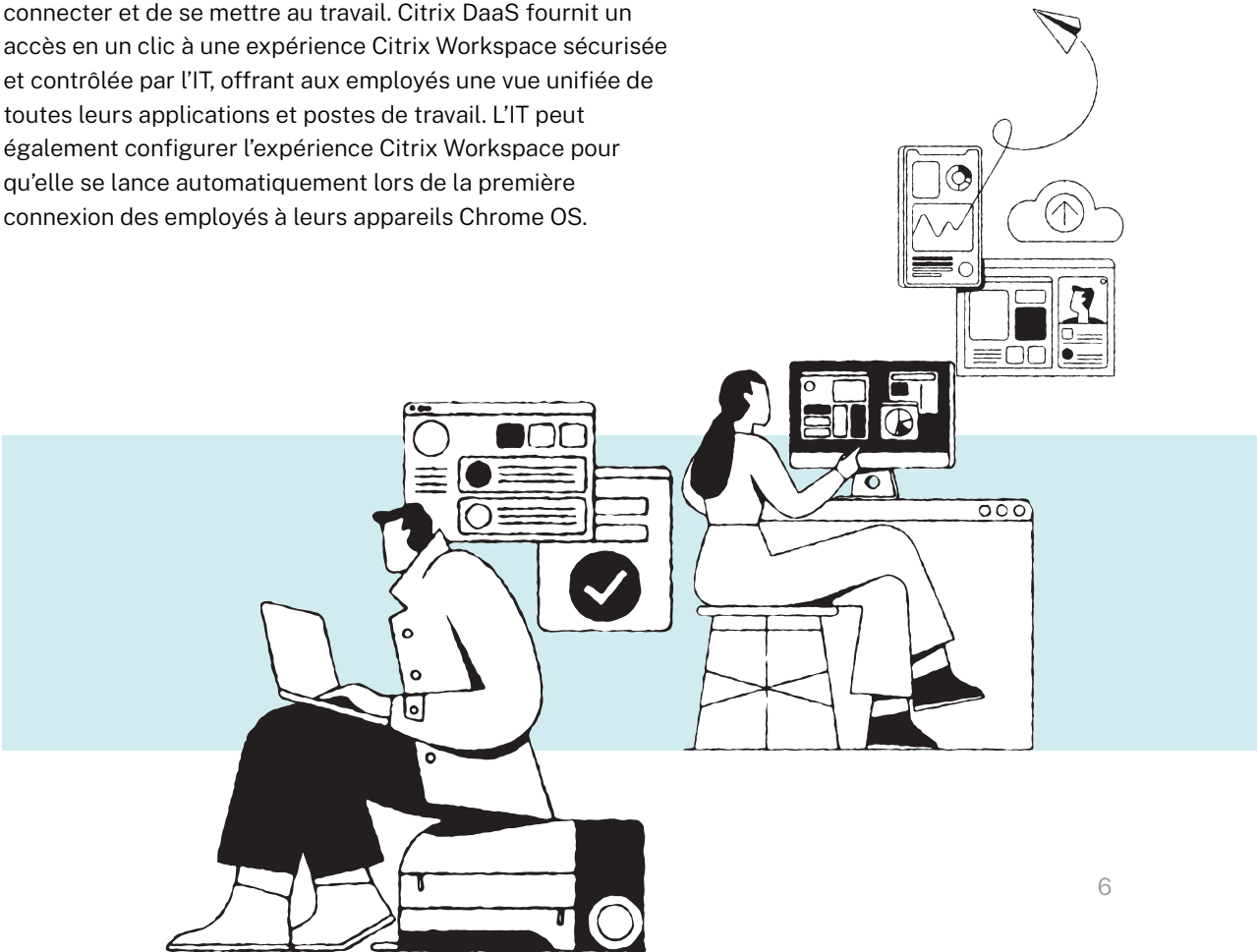
De plus, grâce à l'intégration native de Citrix avec la console de gestion Chrome Enterprise, l'IT peut rapidement provisionner des appareils Chrome OS avec l'application Citrix Workspace sans jamais toucher un appareil. En outre, Citrix Analytics for Security fournit des insights sur les applications, les appareils et les réseaux, et automatise les mesures de sécurité en fonction du comportement des utilisateurs et des autres anomalies détectées.

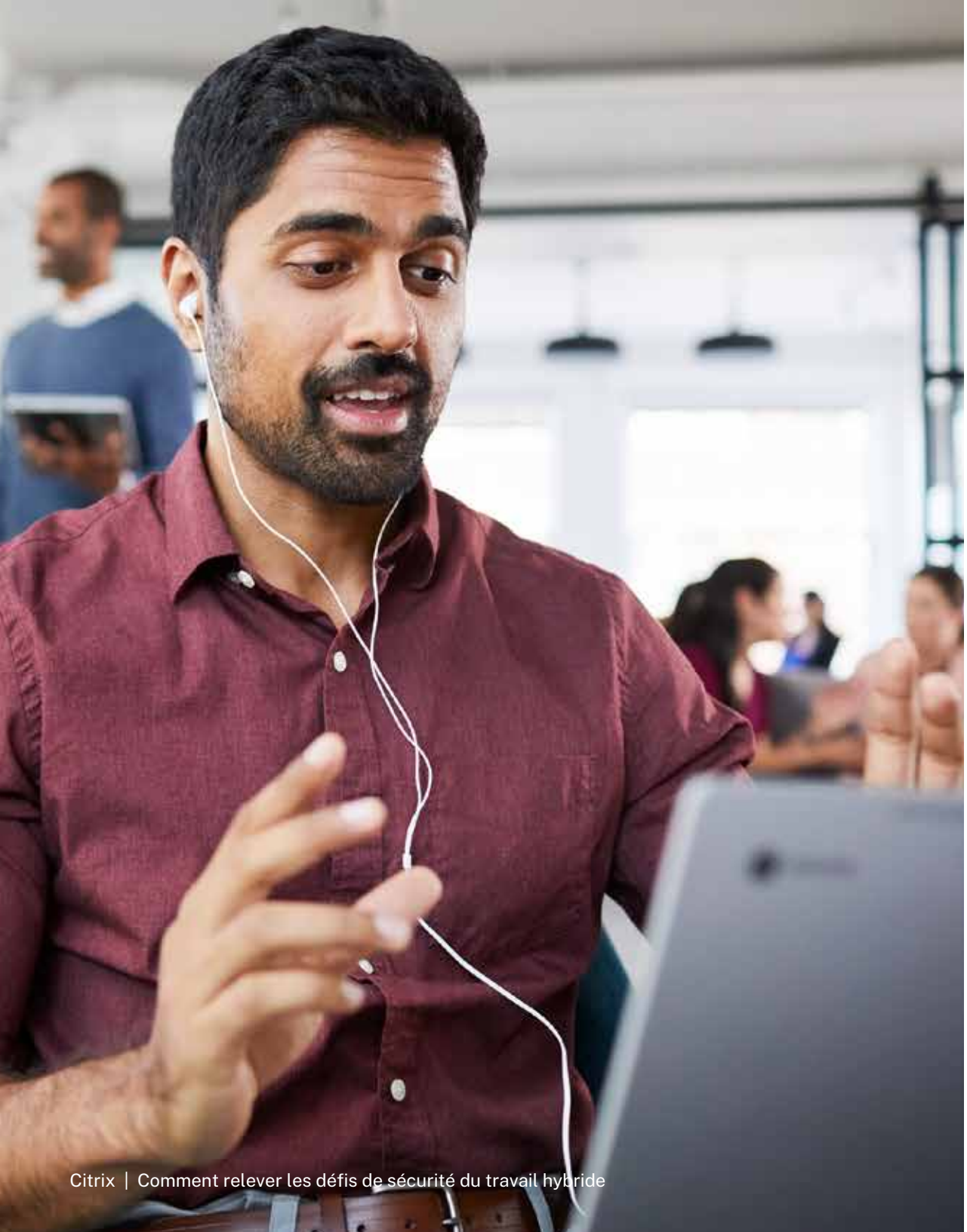
Mettre à disposition n'importe quelle application ou poste de travail

Citrix étend l'accès utilisateur à tous les types d'applications virtuelles sur les appareils Chrome OS, y compris les applications Windows héritées et multifonction, quel que soit le système d'exploitation pour lequel les applications ont été conçues. De même, certains employés peuvent avoir besoin d'utiliser un poste de travail Windows ou Linux traditionnel. L'application Citrix Workspace peut également fournir un accès sécurisé à ces postes depuis n'importe quel appareil Chrome OS.

Offrir une expérience utilisateur exceptionnelle

Pour commencer une nouvelle tâche ou même une journée de travail ordinaire, il suffit d'ouvrir un appareil Chrome OS, de se connecter et de se mettre au travail. Citrix DaaS fournit un accès en un clic à une expérience Citrix Workspace sécurisée et contrôlée par l'IT, offrant aux employés une vue unifiée de toutes leurs applications et postes de travail. L'IT peut également configurer l'expérience Citrix Workspace pour qu'elle se lance automatiquement lors de la première connexion des employés à leurs appareils Chrome OS.





Renforcer la sécurité pour aider les entreprises à se développer

Les solutions Citrix DaaS et Chrome OS aident à créer les expériences d'espace de travail numérique sécurisées dont vos employés ont besoin pour être les plus performants possibles. Que vos équipes travaillent au bureau, à la maison ou en déplacement, elles bénéficient d'une expérience de travail hybride sécurisée qui leur permet de penser, de créer et d'innover.

Donnez à vos employés l'espace nécessaire pour réussir, tout en protégeant votre entreprise. Citrix et Chrome OS évolueront avec vous de façon sécurisée.

En savoir plus sur **Citrix.com/google**

citrix™ chrome OS

Notes de fin de page

[1] Kevin Casey, Hybrid work by the numbers : 14 stats to see
[2] Daniel Newman, The New Normal : Hybrid Work Means Greater Focus On Endpoint Security
[3] Université de Pittsburgh, Laptop and Mobile Device Theft Awareness
[4] Ibid
[5] Google, Free your business from ransomware with Chrome OS