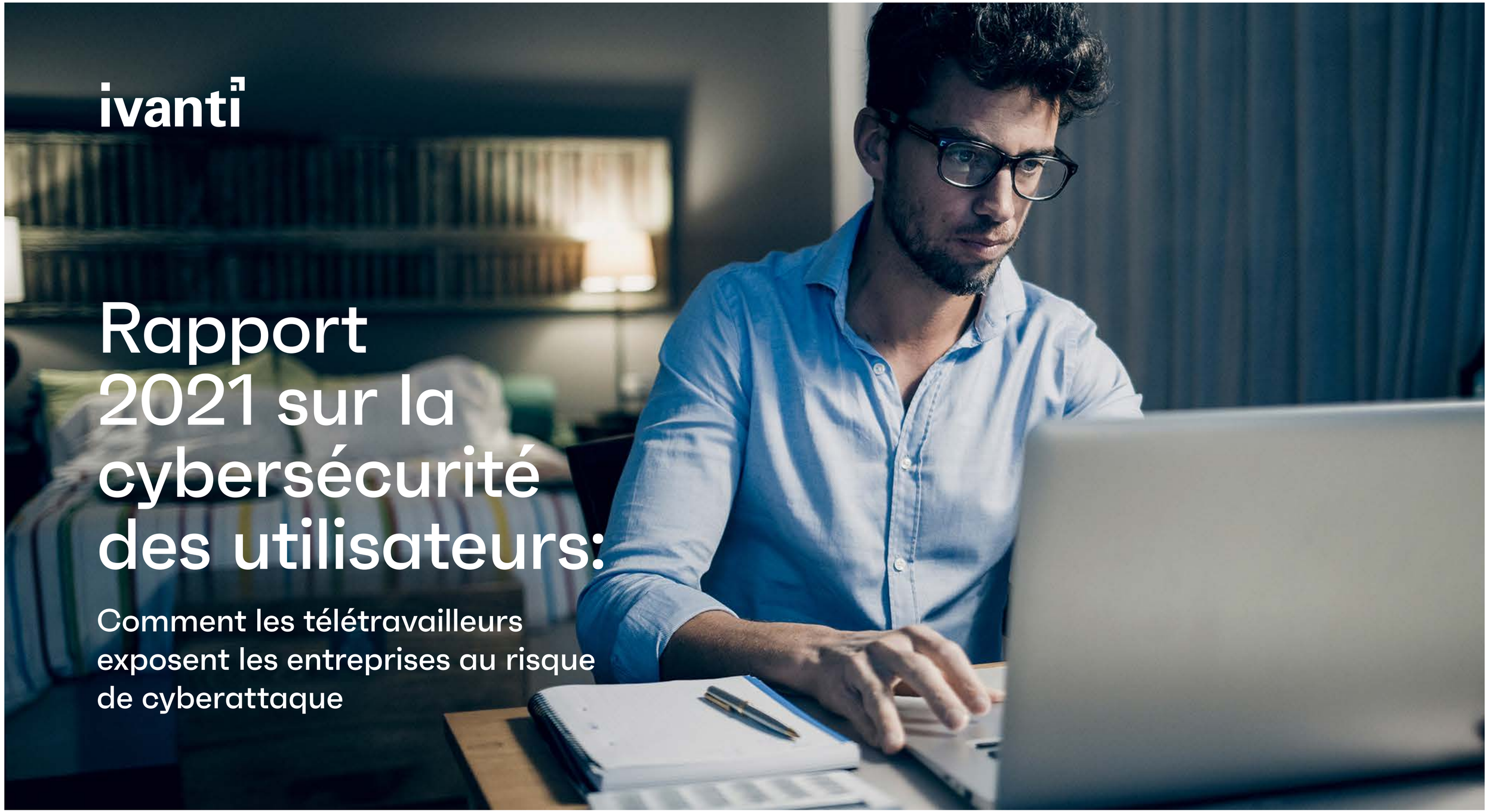
ivanti

Rapport 2021 sur la cybersécurité des utilisateurs:

Comment les télétravailleurs exposent les entreprises au risque de cyberattaque



Les comportements dangereux des utilisateurs accentuent les failles de cybersécurité

La pandémie de 2020, c'est non seulement un virus terrible et mortel qui s'étend dans le monde entier, mais aussi un bouleversement total des aspects essentiels de notre vie quotidienne, notamment de nos lieux et modes de travail. Les collaborateurs de tous types, dans tous les secteurs d'activité, ont commencé à travailler depuis leur domicile autant que possible. Même si ces télétravailleurs ont permis de maintenir les opérations critiques des entreprises, un grand nombre d'entre elles constatent maintenant une augmentation des menaces de cybersécurité, en raison de la multiplication des périphériques personnels non sécurisés et du comportement risqué des collaborateurs. Après plus d'un an de pandémie, à quoi ressemble le paysage des menaces aujourd'hui ?

En février 2021, Ivanti a publié un rapport sur la cybersécurité des utilisateurs (« 2021 Secure Consumer Cyber Report »), qui révèle les menaces spécifiques qui mettent les entreprises en danger. Les résultats reposent sur un panel national représentatif de plus de 2 000 personnes de plus de 18 ans aux États-Unis et au Royaume-Uni, en novembre 2020.

Même si les entreprises ont conscience des vulnérabilités que représentent les périphériques et applications non gérés appartenant aux collaborateurs, ce rapport montre que les collaborateurs ont des comportements très dangereux, même lorsque l'entreprise leur confie un ordinateur pour travailler à domicile. Par exemple, un utilisateur sur quatre a avoué utiliser son adresse e-mail ou son mot de passe d'entreprise pour accéder à des sites web et à des applications grand public, notamment les sites de livraison de repas, les sites d'achats en ligne et même les applications de rencontre.

Une sécurité d'entreprise plus complexe

Même si le monde revient à la situation « normale » d'avant le COVID, le télétravail va probablement perdurer. Bien que les entreprises aient déjà tenté de combler les failles de sécurité chez leurs télétravailleurs, il est évident qu'elles vont devoir faire bien plus que fournir simplement des logiciels et du matériel appartenant à l'entreprise. La lecture attentive des conclusions de ce rapport devrait donner aux entreprises des détails plus complets sur les difficultés qui les attendent.

1 utilisateur sur 4

a avoué utiliser son adresse e-mail ou son mot de passe d'entreprise pour accéder à des sites Web et à des applications grand public, notamment les sites de livraison de repas, les sites d'achats en ligne et même les applications de rencontre.

Les habitudes de sécurité des télétravailleurs mettent leur entreprise en danger

Pour mieux comprendre le niveau de sécurité d'un environnement de télétravail typique, l'enquête a interrogé les personnes du panel sur leur comportement et leurs pratiques de sécurité pour tous leurs périphériques, y compris les périphériques IoT de leur domicile.

Réutilisation des références d'authentification :
Près d'un quart des personnes interrogées aux États-Unis et près d'une sur cinq au Royaume-Uni déclarent avoir utilisé leur adresse e-mail ou leur mot de passe professionnel pour accéder à des sites Web ou des applications grand public.

Utilisation de périphériques personnels pour le travail :
Presque la moitié des Américains et plus d'un tiers des Britanniques interrogés disent qu'ils sont autorisés à se servir d'un périphérique personnel (ordinateur portable, smartphone, tablette ou montre connectée) pour accéder aux applications et aux réseaux de l'entreprise.

Authentification à 2 facteurs pour les périphériques IoT :
Presque la moitié des personnes interrogées (USA comme UK) n'ont pas configuré l'authentification à deux facteurs sur les périphériques intelligents de leur domicile.

Points clés à retenir : N'oubliez pas de mettre en œuvre les pratiques de sécurité de base chez vous

L'absence des garde-fous de sécurité de base sur les périphériques IoT du domicile rend les télétravailleurs et leur entreprise plus vulnérables aux cybermenaces, comme l'attaque Ring, devenue virale en 2019.

Les mauvaises habitudes de sécurité, comme la réutilisation des mots de passe pour l'accès aux sites Web grand public, peuvent augmenter les risques de faille pour l'entreprise. Les entreprises doivent mettre en place une séparation très nette entre les applications et sites Web utilisés pour le travail et les activités personnelles.

Également, manque de sécurité d’entreprise pour l’ensemble des télétravailleurs

Après le début de la pandémie, l’on a constaté une augmentation dramatique des attaques de cybersécurité visant des périphériques personnels non sécurisés et les périphériques IoT du domicile. Même si les mauvaises habitudes de sécurité de la part des utilisateurs finaux sont en partie responsables, notre enquête a montré que les entreprises devraient également renforcer leur sécurité sur certains points essentiels.

25%

Logiciels de sécurité :
Plus d’un quart des personnes interrogées déclarent qu’on ne leur a imposé aucun logiciel de sécurité spécifique sur leurs périphériques, pour l’accès à certaines applications dans le cadre du télétravail.

Mise à jour des mots de passe :
Environ 25 % des télétravailleurs, aussi bien aux États-Unis qu’au Royaume-Uni, disent que leur entreprise ne leur impose pas de mettre à jour leur mot de passe tous les six mois, ni d’utiliser un générateur de mots de passe à usage unique.

30%

Outils d’accès sécurisé :
Environ 30 % des personnes interrogées, aux États-Unis comme au Royaume-Uni, disent que leur entreprise n’impose pas aux télétravailleurs l’emploi d’un outil d’accès sécurisé comme le VPN.

Points clés à retenir : La sécurité « Zero Trust » est indispensable

Le télétravail est là pour rester. Même si les départements IT d’entreprise ont amélioré la sécurité mobile dans certains domaines, ils doivent encore renforcer l’authentification sécurisée sur tous les périphériques que les collaborateurs utilisent pour travailler.

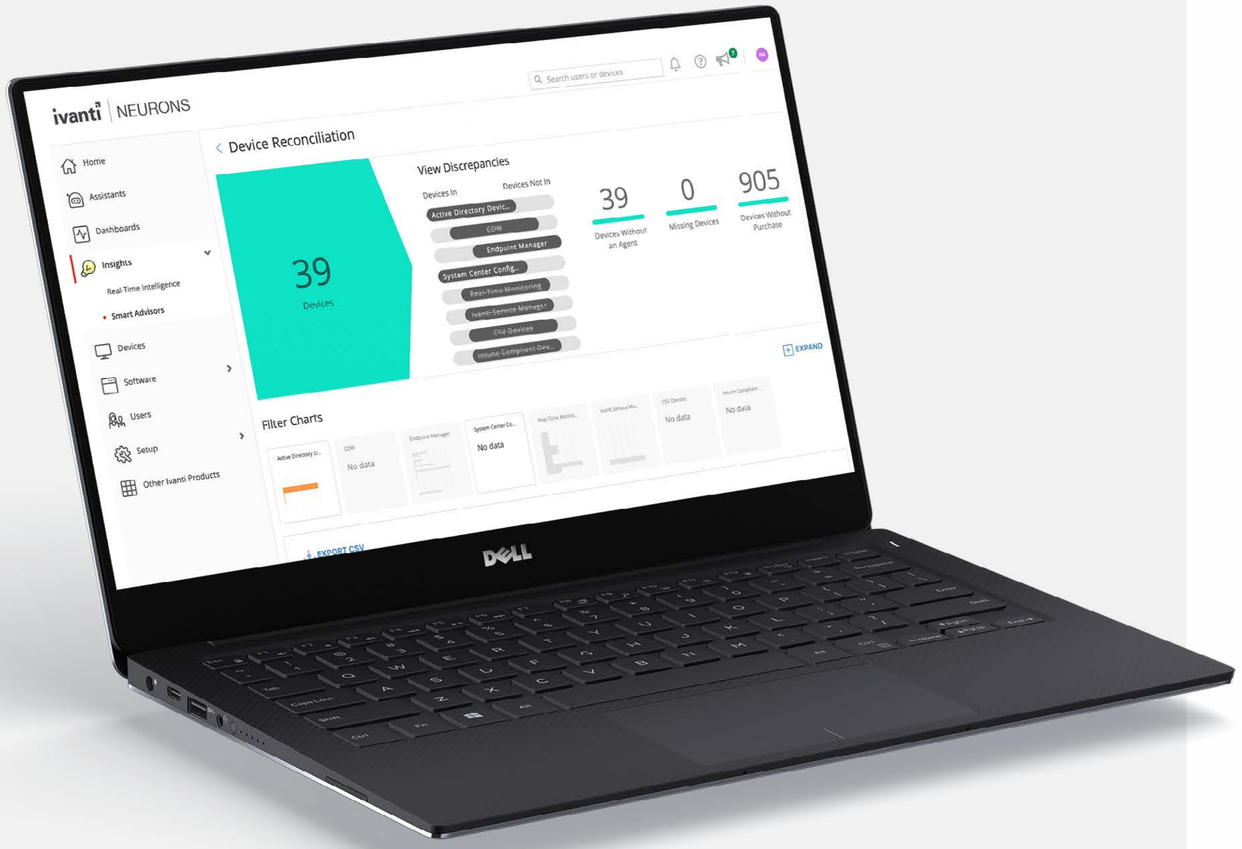
Une structure Zero Trust, qui permet la vérification transparente, automatisée et constante de tous les utilisateurs, périphériques, applications, réseaux et Clouds, est indispensable pour réellement sécuriser l’Everywhere Workplace.

Sécuriser les utilisateurs pour sécuriser les entreprises

Maintenant que les télétravailleurs sont plus nombreux que jamais, le paysage des menaces s'étend comme jamais auparavant. C'est pourquoi les entreprises doivent mettre en place des stratégies essentielles pour protéger les applications et les données métier contre les failles de sécurité IoT et le comportement des utilisateurs à leur domicile. Il est évident que plus les périphériques grand public se multiplient, plus les télétravailleurs ont du mal à activer et à maintenir des paramètres de sécurité avancés… et les cybercriminels le savent. Ainsi, en plus de représenter une menace mondiale pour la santé des humains, la pandémie de COVID-19 menace également notre bien-être, car elle permet à des cybercriminels de tirer plus facilement profit des personnes et des entreprises qui ne sont pas suffisamment protégées.

Bonne nouvelle, cependant : Les entreprises peuvent mettre en place une sécurité Zero Trust dès maintenant

Les entreprises peuvent prendre des mesures pour commencer à implémenter des protocoles Zero Trust pour l'ensemble de leurs télétravailleurs. En mettant en place un modèle Zero Trust, les entreprises évitent tout risque de vol des références d'authentification, car le système vérifie que tous les accès aux informations, applications ou réseaux de l'entreprise proviennent d'une entité de confiance. En outre, si le télétravail persiste et que les périphériques continuent à se multiplier, la sécurité Zero Trust facilitera grandement la mise en place de stratégies d'utilisation admise, notamment l'utilisation de l'authentification à deux facteurs, la protection des périphériques et les connexions réseau sécurisées.



Méthodologie

Les conclusions du rapport initial sur la cybersécurité des utilisateurs (« Secure Consumer Cyber Report ») sont basées sur une enquête menée en novembre 2020. Cette étude visait à découvrir comment les habitudes de cybersécurité des utilisateurs et des entreprises ont changé depuis le début de la pandémie. L'enquête portait sur un panel représentatif national de 2 000 résidents des États-Unis et du Royaume-Uni âgés de plus de 18 ans, qui travaillaient depuis leur domicile sur un ordinateur fourni par l'entreprise.

À propos d'Ivanti

La plateforme d'automatisation Ivanti rend toutes les connexions IT plus intelligentes et plus sûres pour tous les périphériques, infrastructures distantes et utilisateurs. Des PC ou périphériques mobiles au VDI et au data center, Ivanti permet de découvrir, de gérer et de sécuriser les biens IT, et de leur fournir des services, du Cloud à la périphérie dans l'Everywhere Workplace, tout en offrant une expérience personnalisée aux collaborateurs. Dans l'Everywhere Workplace, les données d'entreprise transitent librement entre les différents périphériques et serveurs, ce qui permet aux utilisateurs d'être productifs partout, quelle que soit la façon dont ils travaillent. Le siège social d'Ivanti se trouve à Salt Lake City, dans l'Utah (États-Unis). La société compte des filiales dans le monde entier. Pour en savoir plus, visitez le site www.ivanti.fr et suivez @GoIvanti.

ivanti

ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr