HP WOLF SECURITY

TRAVAIL HYBRIDE & CYBERSÉCURITÉ : LA FRONTIÈRE ÉTROITE ENTRE USAGES PERSONNELS ET PROFESSIONNELS

SYNTHÈSE ET RÉSULTATS CLÉS

Parmi les nombreux effets de la pandémie de COVID-19 sur les entreprises, l'un des plus importants a été le fait que plusieurs centaines de millions d'employés ont dû adopter le télétravail. Début 2020, le télétravail est passé en quelques semaines d'une méthode de travail occasionnelle pratique pour les employés au seul moyen permettant à de nombreuses entreprises de continuer à fonctionner.

L'échelle de ce changement a été incomparable. Une enquête YouGov réalisée auprès d'employés de bureau du monde entier à la demande de HP dans le cadre de ce rapport indique que 82 % d'entre eux travaillent plus fréquemment depuis chez eux depuis le début de la pandémie. Cette situation a entraîné une réévaluation du télétravail et de ses avantages irréfutables sur le plan économique comme personnel. Il semble probable que les tendances de travail évolueront de manière permanente, ce à quoi les entreprises devront s'adapter afin de conserver leur avantage concurrentiel. En effet, il a été prouvé que 23 % des employés de bureau du monde entier s'attendaient à travailler principalement depuis chez eux une fois la pandémie terminée, et que 16 % supplémentaires prévoyaient de partager leur temps entre le télétravail depuis leur domicile et le travail au bureau.

Mais un danger existe : que les entreprises adoptent le télétravail sans analyser comment cet environnement amplifie les menaces existantes sur le plan de la sécurité. La quantité de données professionnelles, y compris de documents financiers sensibles, consultées depuis le domicile d'employés a augmenté de manière significative, exposant ainsi au risque davantage d'informations. Dans le même temps, le nombre de terminaux – personnels et fournis par l'employeur – utilisés pour accéder au réseau de l'entreprise au-delà du périmètre traditionnellement établi a explosé.

Les données de ce rapport mettent en lumière les limites du modèle de sécurité périmétrique pour la sécurisation des télétravailleurs, ainsi que le fardeau qu'il représente pour les équipes responsables de la sécurité. Souvent, les terminaux comme les ordinateurs portables, PC et imprimantes restent exposés, ce qui augmente les chances que les problèmes de sécurité restent invisibles jusqu'à ce que des dégâts soient constatés. À cause de ces points faibles, beaucoup d'entreprises sont potentiellement exposées à des risques importants.

HP Wolf Security[1] est notre nouveau portefeuille intégré de matériel, logiciels et services de sécurité, spécialement conçu pour cette nouvelle normalité. Dans ce rapport HP Wolf Security, nous présentons de manière multidimensionnelle les problèmes de sécurité existants. Celui-ci combine également les résultats d'une enquête en ligne YouGov effectuée auprès de 8 443 employés de bureau du monde entier ayant adopté le télétravail pendant la pandémie, et d'une étude mondiale à laquelle ont participé 1 100 décisionnaires IT, afin d'analyser tous les aspects de la situation. Ces données sont également enrichies grâce à des données télémétriques liées aux menaces existant dans le monde réel et provenant de machines virtuelles équipées de HP Sure Click – afin de démontrer ces risques – ainsi que des analyses de pointe effectuées par KuppingerCole permettant d'illustrer le contexte mondial.

En examinant la situation sous ces différents angles, ce rapport HP Wolf Security se penchera sur :

01 **Comment le monde a changé avec l'émergence des « nouveaux bureaux »**, en analysant l'accélération de la transition vers le télétravail et comment cette dernière a fait des terminaux une première ligne de défense.

02 **L'impact de la pandémie sur les attitudes et comportements des utilisateurs,** en montrant que les employés prennent plus de risques qu'ils n'en prendraient au bureau. Ceux-ci deviennent ainsi des « ennemis amicaux » sans le vouloir, et font augmenter les risques de violations de données involontaires.

03 **La pression que crée cette situation sur les spécialistes en cybersécurité avec l'émergence de nouvelles menaces.** La multiplication croissante de terminaux, y compris d'appareils connectés (IoT), accroît la surface d'attaque pour les personnes cherchant à pénétrer dans les réseaux d'entreprises.

04 **Pourquoi une nouvelle génération de solutions de sécurité des terminaux, comme HP Wolf Security, est nécessaire pour se protéger contre les menaces modernes,** en démontrant comment un alignement avec les principes d'une approche de confiance zéro (Zero Trust) aidera votre entreprise à réduire la surface d'attaque, minimiser les risques et mieux soutenir les équipes IT sur-sollicitées.

91 %

des décisionnaires IT estiment que la sécurité des terminaux est devenue aussi importante que la sécurité réseau, et autant déclarent accorder plus de temps à la sécurité des terminaux qu'il y a deux ans.

76 %

des employés de bureau déclarent que le télétravail depuis leur domicile pendant la pandémie de COVID-19 a flouté les frontières existant entre leur vie personnelle et leur vie professionnelle. La moitié d'entre eux déclarent qu'ils considèrent aujourd'hui leur appareil de travail comme un appareil personnel, et 46 % admettent utiliser leur ordinateur portable de travail pour un usage personnel au quotidien.

30 %

des employés ont laissé une autre personne utiliser leur appareil de travail, malgré le fait que 85 % des décisionnaires IT déclarent craindre qu'un tel comportement augmente les risques de violations de sécurité pour leur entreprise.

54 %

des décisionnaires IT déclarent avoir constaté plus d'attaques de hameçonnage au cours de l'année passée, et 45 % ajoutent avoir vu des imprimantes compromises utilisées comme point d'attaque au cours de cette même période.

1
LE NOUVEAU BUREAU

71 % DES EMPLOYÉS ACCÈDENT PLUS SOUVENT À PLUS DE DONNÉES APPARTENANT À LEUR ENTREPRISE DEPUIS CHEZ EUX QU'AVANT LA PANDÉMIE.

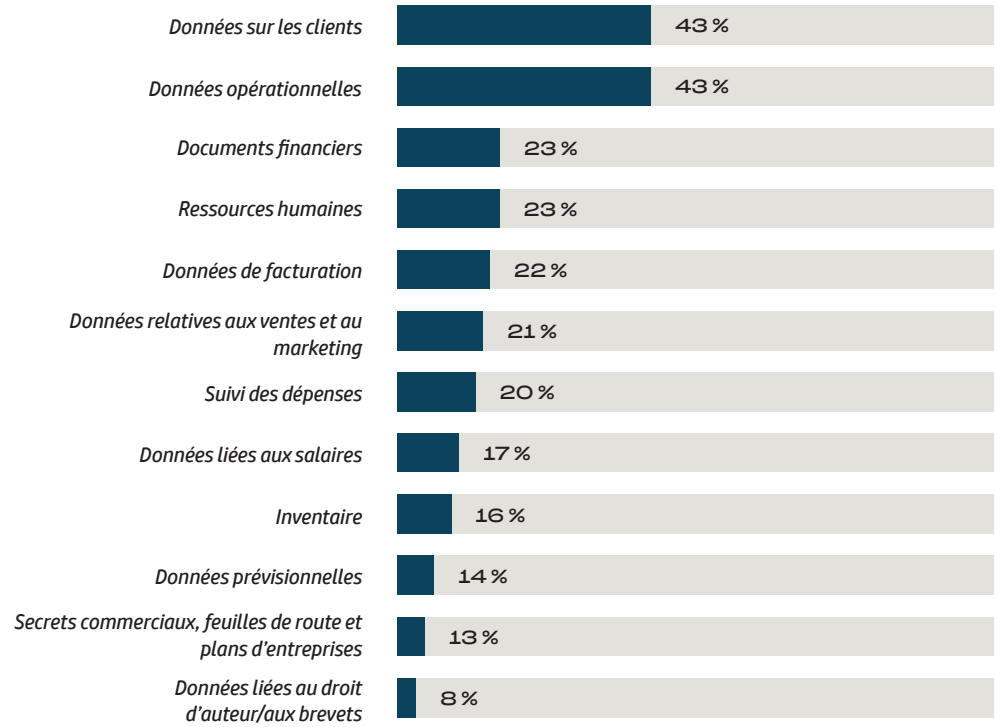
POINT DE VUE HP WOLF SECURITY :

IAN PRATT, DIRECTEUR DE LA SÉCURITÉ, PERSONAL SYSTEMS, HP INC. :

« Les méthodes traditionnelles de sécurisation de l'accès au réseau, aux applications et aux données des entreprises ne sont plus adaptées. La sécurité périmétrique est devenue obsolète. Au fil du temps, les équipes sont devenues plus dispersées et l'adoption des solutions SaaS a augmenté. Cela signifie que les données critiques sont hébergées en dehors du pare-feu de l'entreprise. Le moment est donc venu pour les entreprises de commencer à se protéger contre les menaces inconnues, en utilisant une approche « Zero Trust », mais de manière transparente pour les utilisateurs. »

LE NOMBRE DE CYBERATTAQUES MONDIALES A AUGMENTÉ DE 238 % ENTRE FÉVRIER ET AVRIL 2020.

Si la pandémie n'a pas donné naissance à la tendance du télétravail et des environnements de travail hybrides partagés entre le domicile et le bureau, elle a grandement accéléré son adoption, condensant en quelques mois seulement l'équivalent d'une décennie potentielle d'évolution progressive vers un environnement de travail à distance et mobile. Cette situation a entraîné un résultat inévitable : le besoin accru pour les employés d'accéder à distance aux données de leur entreprise. Ce rapport HP Wolf Security montre que 71 % des employés de bureau interrogés accèdent plus souvent à plus de données appartenant à leur entreprise depuis chez eux qu'avant la pandémie, et les types de données les plus couramment consultées incluent notamment :



Les cybercriminels ont rapidement profité du chaos. Comme pour la pandémie, les cyberattaques apparaissent par vagues, en commençant par une phase initiale lors de laquelle les criminels réalisent que les entreprises sont plus vulnérables aux attaques qu'auparavant. Selon des statistiques du Forum économique mondial (FEM), le nombre de cyberattaques mondiales a augmenté de 238 % entre février et avril 2020.

Repousser de telles attaques est de plus en plus difficile car les employés travaillant à distance ne sont plus protégés par le pare-feu de leur entreprise, et beaucoup d'entre eux accèdent à des données critiques via des connexions non sécurisées. Parmi les décisionnaires IT interrogés dans le cadre de cette enquête, 89 % sont préoccupés par le fait que les employés n'utilisent pas une connexion sécurisée, comme un VPN.

CERTAINS SECTEURS SONT PLUS CIBLÉS QUE D'AUTRES :

une augmentation de 50 % des attaques touchant le secteur de la santé a été constatée entre février et mai, et l'Organisation mondiale de la santé (OMS) rapporte une augmentation de 400 % des cyberattaques au cours de la même période.

Les cyberattaques ciblant le secteur de l'éducation ont augmenté de 33 % entre 2019 et 2020.

Le secteur des jeux vidéo a également relevé une augmentation de 54 % des attaques de hameçonnage au cours des premiers mois de l'année 2020.

91 % DES DÉCISIONNAIRES IT DÉCLARENT ACCORDER PLUS DE TEMPS À LA SÉCURITÉ DES TERMINAUX QU'IL Y A DEUX ANS.

En termes de sécurité, l'attention auparavant portée au réseau est désormais portée aux terminaux. L'enquête réalisée auprès des décisionnaires IT a révélé que 91 % d'entre eux estiment que la sécurité des terminaux est devenue aussi importante que la sécurité réseau maintenant que les employés sont plus nombreux à travailler depuis chez eux. De plus, 90 % de ces derniers s'accordent également à dire que la pandémie de 2020 a mis en lumière l'importance croissante d'une sécurité robuste pour les terminaux afin de défendre les entreprises s'appuyant de moins en moins sur une sécurité périmétrique ; 91 % d'entre eux déclarent accorder plus de temps à la sécurité des terminaux qu'il y a deux ans.

Illustration 1 - Pourcentage de décisionnaires IT par pays qui estiment que la sécurité des terminaux est devenue aussi importante que la sécurité réseau en raison du nombre plus important d'employés en télétravail depuis leur domicile

MONDIAL	CANADA	MEXIQUE	ÉTATS-UNIS	ALLEMAGNE	ROYAUME-UNI	JAPON	AUSTRALIE
91 %	91 %	97 %	92 %	85 %	91 %	92 %	92 %

PLUS DE LA MOITIÉ (56 %) DES IMPRIMANTES SONT ACCESSIBLES VIA DES PORTS OUVERTS COURAMMENT UTILISÉS QUI POURRAIENT ÊTRE PIRATÉS.

La nature des terminaux évolue et se diversifie constamment. Selon KuppingerCole : *« Les nombreux appareils connectés utilisés par les employés dans le cadre de télétravail depuis leur domicile ont contribué à la détérioration de l'infrastructure IT et du réseau des entreprises, y compris les imprimantes. »* Les environnements de travail à domicile comptent désormais de nombreux appareils ciblés par les cybercriminels, comme les appareils connectés, connus pour posséder des fonctionnalités de sécurité faibles, comme le souligne KuppingerCole. Ces derniers incluent les imprimantes, qui sont souvent ignorées par les équipes responsables de la sécurité. Une étude réalisée en 2020 et citée par KuppingerCole a en effet démontré que plus de la moitié (56 %) sont accessibles via des ports ouverts couramment utilisés etsusceptibles d'être piratés.

2

LE DILEMME DES « ENNEMIS AMICAUX »

POINT DE VUE HP :

JOANNA BURKEY, RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI), HP INC. :

« Comme les employés travaillent à distance, la différence entre équipement professionnel et personnel devient floue, et des actions du quotidien – comme ouvrir une pièce jointe – peuvent avoir de sérieuses conséquences. Sans toutes les sources de visibilité sur les appareils que nous possédions avant la pandémie, y compris comment ceux-ci sont utilisés et par qui, les équipes IT et en charge de la sécurité travaillent à l'aveugle. »

PARMI LES PERSONNES AYANT PARTAGÉ LEUR APPAREIL, 27 % DÉCLARENT SAVOIR QU'ELLES NE SONT PAS SUPPOSÉES LE FAIRE, MAIS ESTIMENT « NE PAS AVOIR LE CHOIX » EN RAISON DE LA SITUATION EXCEPTIONNELLE ACTUELLE.

L'adoption du télétravail à domicile a transformé la nature et l'échelle des risques liés à la cybersécurité. Au sein de nombreuses entreprises, ce changement n'a pas encore été pleinement mesuré, souvent parce qu'il est moins visible ou sous-estimé. Une facette intéressante de cette évolution est le changement culturel constaté. Un appareil utilisé au bureau vit une existence relativement insipide. Emportez ce même appareil dans un environnement de travail à domicile, et tout change. Chez eux, les employés font des choses qu'ils ne feraient jamais au bureau, ce qui peut rapidement multiplier les risques liés à la cybersécurité de nombreuses manières difficiles à contrôler.

Preuve de ce problème, le rapport HP Wolf Security montre que 76 % des employés de bureau interrogés déclarent que le télétravail depuis leur domicile pendant la pandémie de COVID-19 a flouté les frontières existant entre leur vie personnelle et leur vie professionnelle, mélangeant ainsi travail et vie privée dans un environnement unique. Lorsqu'ils sont interrogés sur la manière dont tout cela influence leur utilisation de leurs appareils professionnels, 50 % s'accordent à dire qu'ils considèrent désormais leur ordinateur portable de travail comme un appareil personnel.

Illustration 2 - Pourcentage d'employés de bureau par pays qui déclarent que le télétravail depuis leur domicile pendant la pandémie de COVID-19 a flouté les frontières existant entre leur vie personnelle et leur vie professionnelle

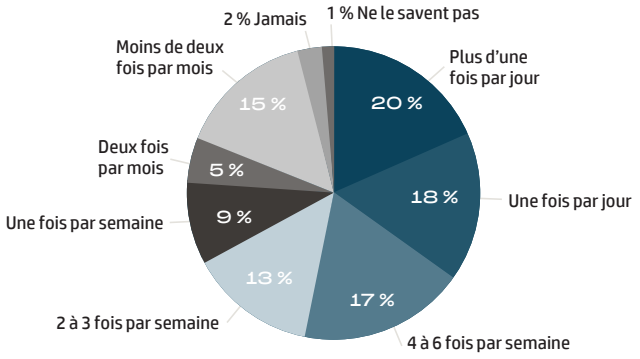
MONDIAL	CANADA	MEXIQUE	ÉTATS-UNIS	ALLEMAGNE	ROYAUME-UNI	JAPON	AUSTRALIE
76 %	78 %	84 %	77 %	78 %	79 %	62 %	77 %

De plus, et potentiellement plus problématique, 30 % d'entre eux avouent également avoir déjà autorisé quelqu'un d'autre qu'eux – comme un(e) partenaire, enfant ou ami(e) – à utiliser leur ordinateur portable de travail, souvent plus d'une fois par jour. Parmi les personnes ayant partagé leur appareil, 27 % déclarent savoir qu'elles ne sont pas supposées le faire, mais estimaient « ne pas avoir le choix » en raison de la situation exceptionnelle actuelle.

Illustration 3

Région	% des employés de bureau qui déclarent commencer à considérer leur notebook/ordinateur portable de travail comme leur notebook/ordinateur portable de travail ***et*** personnel depuis qu'ils travaillent chez eux	% des employés de bureau qui déclarent que quelqu'un d'autre qu'eux a déjà utilisé leur ordinateur portable ou PC de travail au cours de l'année passée
MONDIAL	50 %	30 %
CANADA	63 %	37 %
MEXIQUE	79 %	55 %
ÉTATS-UNIS	53 %	31 %
ALLEMAGNE	30 %	16 %
ROYAUME-UNI	33 %	12 %
JAPON	35 %	21 %
AUSTRALIE	59 %	34 %

Illustration 4 - Fréquence moyenne à laquelle des PC ou ordinateurs portables professionnels sont utilisés par quelqu'un d'autre



84 % DES DÉCISIONNAIRES IT SONT PRÉOCCUPÉS PAR LE FAIT QUE LES EMPLOYÉS QUI UTILISENT LEURS APPAREILS DE TRAVAIL DANS UN CADRE PERSONNEL AU COURS DE LA PANDÉMIE EXPOSENT LEUR ENTREPRISE À DE PLUS GRANDS RISQUES DE VIOLATION DE SÉCURITÉ.

La conséquence de ce sentiment de propriété des appareils est que les employés se préoccupent de moins en moins des risques de sécurité et utilisent de plus en plus ces appareils de travail pour un usage personnel : 84 % des décisionnaires IT sont préoccupés par le fait que les employés utilisant leurs appareils de travail dans un cadre personnel au cours de la pandémie exposent leur entreprise à de plus grands risques de violation de sécurité.

Quand on les interroge, les décisionnaires IT estiment qu'environ un tiers (33 %) de leurs employés utilisent leur ordinateur de travail pour un usage personnel (comme pour jouer à des jeux, naviguer sur Internet, etc.), alors que ce chiffre est en réalité bien plus élevé. 70 % des employés de bureau interrogés admettent utiliser leur appareil de travail, ou laisser quelqu'un d'autre l'utiliser, pour un usage personnel ; 46 % admettent même utiliser leur ordinateur portable de travail pour un usage personnel au quotidien, chiffre qui s'élève à 61 % chez les personnes âgées de 25 à 34 ans. Quatre employés de bureau sur dix interrogés admettent utiliser leur appareil professionnel pour des devoirs et cours en ligne, statistique atteignant 57 % chez les parents d'enfants de 5 à 16 ans.

De nombreux autres comportements à risque sont fréquemment constatés. Les employés de bureau interrogés (ou les personnes vivant dans le même foyer) ont reconnu avoir utilisé des ordinateurs portables de travail pour les tâches personnelles suivantes :

- *Téléchargements sur Internet : 33 %*
- *Consultation de pièces jointes d'e-mails ou de pages web personnelles : 55 %*
- *Consultation de pages de réseaux sociaux personnels : 45 %*
- *Appels vidéo : 58 %*
- *Jeux : 27 %*
- *Utilisation de services de streaming en ligne : 36 %*
- *Achats en ligne/navigation sur Internet : 52 %*

L'analyse KuppingerCole étaye ces données, montrant en effet :

- Une augmentation de 36 % du temps de jeu mondial en 2020. Les téléchargements de jeux ont connu une augmentation allant jusqu'à 80 %, selon les sorties récentes de jeux vidéo.
- Une augmentation de 54 % des exploitations des plateformes de jeux populaires par des personnes mal intentionnées entre janvier et avril 2020, redirigeant souvent les utilisateurs vers des pages de hameçonnage.

Menaces liées aux jeux vidéo

En 2020, les données télémétriques liées à Sure Click et Sure Click Enterprise ont démontré une augmentation des malwares liés aux jeux vidéo, en particulier à des titres populaires comme Fortnite et Among Us.

- Exemple notable : le rançongiciel Ryuk dissimulé sous la forme de cheats pour Fortnite (« FreeHacks4Fortnite.exe »). Sure Click Enterprise a permis d'identifier les utilisateurs téléchargeant et utilisant des fichiers provenant de Mega, un site de partage de fichiers. Sure Click Enterprise a ensuite permis d'isoler ces fichiers avec succès et d'éviter que ces malwares ne provoquent un chiffrement de l'appareil concerné.

En février 2021, Sure Click a isolé des fragments d'un outil de téléchargement de malwares JavaScript appelé Gootloader.

- Celui-ci présentait un taux de détection très faible sur VirusTotal, et échappait souvent à tous les moteurs de détection.
- Certains fragments étaient dissimulés sous la forme de hacks pour Fortnite.
- Contenu dans des archives zip.
- Éléments finaux : Gootkit (cheval de Troie bancaire) ou REvil (rançongiciel).

Menace liée aux e-mails personnels

En 2020, HP Sure Click et Sure Click Enterprise ont permis d'empêcher 128 utilisateurs de télécharger des fichiers infectés issus de services de courrier électronique personnel non protégés par des filtres professionnels, dont des malwares Emotet et rançongiciels.

Menaces liées au streaming

D'après l'analyse de KuppingerCole, les services de streaming ont également été ciblés pendant la pandémie, avec au moins 700 sites frauduleux se faisant passer pour des services de streaming populaires ayant été identifiés au cours d'une période de 7 jours en avril 2020. Les attaques de hameçonnage visant les utilisateurs de Netflix ont augmenté de 60 % par rapport à 2019. Les URL de hameçonnage ciblant Netflix ont augmenté de 646 % par rapport à 2019, celles ciblant Twitch ont augmenté de 337 %, celles ciblant HBO ont augmenté de 525 % et celles ciblant YouTube ont augmenté de 3 064 %.

69 % DES EMPLOYÉS DE BUREAU ONT DÉJÀ UTILISÉ LEUR ORDINATEUR PORTABLE OU IMPRIMANTE/ SCANNER PERSONNEL(LE) POUR DES TÂCHES LIÉES À LEUR TRAVAIL DEPUIS LE DÉBUT DE LA PANDÉMIE.

Une autre tendance claire a été constatée : les employés accèdent aux réseaux professionnels grâce à leurs appareils personnels. Dans le cadre de cette enquête, les décisionnaires IT estiment qu'un peu plus de la moitié (53 %) de leurs employés utilisent des appareils personnels pour les tâches liées à leur travail. Encore une fois, le chiffre réel est plus élevé : ce rapport HP Wolf Security montre que 69 % des employés de bureau interrogés ont déjà utilisé leur ordinateur portable ou imprimante/scanner personnel(le) pour des tâches liées à leur travail depuis le début de la pandémie. Ces derniers utilisent leurs appareils personnels pour un large éventail de tâches plus fréquemment depuis l'année passée :

- *34 % d'entre eux utilisent l'imprimante de leur domicile pour numériser et partager des documents avec des collègues et clients*
- *21 % d'entre eux utilisent leur imprimante personnelle pour sauvegarder des fichiers via le VPN*
- *37 % d'entre eux utilisent leur PC/ordinateur portable personnel pour accéder à des applications de travail*
- *35 % d'entre eux utilisent leur PC/ordinateur portable personnel pour enregistrer des documents professionnels*
- *27 % d'entre eux utilisent leur téléphone portable pour transférer des documents professionnels vers l'imprimante de leur domicile*
- *32 % d'entre eux utilisent leur PC/ordinateur portable personnel pour accéder au réseau principal de leur entreprise*

3
L'EXPLOSION DES MENACES

Le danger de ces nouveaux comportements vis-à-vis de la technologie est que les entreprises se retrouvent face à des risques sur lesquels elles n'ont plus aucune visibilité. L'enquête réalisée auprès des décisionnaires IT dans le cadre du rapport HP Wolf Security met clairement en lumière les inquiétudes de ces derniers concernant ce point. En effet, plus d'un tiers (35 %) d'entre eux déclarent que les difficultés à contrôler l'utilisation des appareils de l'entreprise et l'impossibilité de superviser qui les utilise sont leurs plus grands problèmes actuels. Les décisionnaires IT ont déclaré être préoccupés par certains nouveaux comportements d'employés, qui selon eux augmentent les risques pour l'entreprise :

- 85 % d'entre eux craignent que le fait que les employés laissent d'autres personnes (des enfants, partenaires, colocataires, etc.) utiliser leurs appareils professionnels augmente les risques de violation de sécurité pour leur entreprise.
- 88 % d'entre eux craignent que le fait que les employés téléchargent des logiciels (pour faire leur travail) non approuvés par le département IT augmente les risques de violation de sécurité pour leur entreprise.
- 88 % d'entre eux craignent que les risques de violation de données augmentent en raison du fait que les employés utilisent leurs appareils personnels non conçus pour une sécurité professionnelle dans le cadre de leur travail.

Illustration 5

Région	% des décisionnaires IT qui estiment que le fait que les employés laissent d'autres personnes utiliser leurs appareils professionnels augmente les risques de violation de sécurité pour leur entreprise	% des décisionnaires IT qui estiment que le fait que les employés téléchargent des logiciels (pour faire leur travail) non approuvés par le département IT augmente les risques de violation de sécurité pour leur entreprise	% des décisionnaires IT qui estiment que le fait que les employés utilisent leurs appareils personnels non conçus pour une sécurité professionnelle dans le cadre de leur travail augmente les risques de violation de sécurité pour leur entreprise
MONDIAL	85 %	88 %	88 %
CANADA	91 %	97 %	95 %
MEXIQUE	87 %	95 %	93 %
ÉTATS-UNIS	83 %	87 %	89 %
ALLEMAGNE	67 %	72 %	71 %
ROYAUME-UNI	87 %	89 %	87 %
JAPON	94 %	93 %	93 %
AUSTRALIE	83 %	87 %	89 %

Et ces inquiétudes sont légitimes. Parmi les décisionnaires IT interrogés, 51 % d'entre eux déclarent avoir constaté l'utilisation d'appareils personnels compromis pour accéder aux données des entreprises et de leurs clients au cours de l'année passée ; 45 % d'entre eux ont également constaté l'utilisation d'imprimantes compromises comme point d'attaque au cours de la même période.

De plus, 54 % de ces décisionnaires IT rapportent avoir remarqué un nombre plus important d'attaques de hameçonnage au sein de leur entreprise au cours de l'année passée ; 56 % ont également constaté une augmentation des attaques liées aux navigateurs web, et 51 % déclarent avoir vu des utilisateurs utiliser des terminaux non protégés au cours de l'année passée.

Illustration 6 - Pourcentage de décisionnaires IT ayant constaté des preuves de ces violations de sécurité au cours de l'année passée

Augmentation des infections liées au hameçonnage	54 %
Augmentation des infections liées aux navigateurs web	56 %
Appareils compromis utilisés pour infecter l'entreprise à plus grande échelle	44 %
Appareils personnels compromis utilisés pour accéder aux données de l'entreprise et des clients	51 %
Utilisateurs utilisant des machines non protégées	51 %
Imprimantes compromises utilisées comme points d'attaque	45 %

POINT DE VUE HP WOLF SECURITY :

ROZ HO, DIRECTRICE MONDIALE DU DÉPARTEMENT LOGICIELS, HP INC. :

« Alors que les entreprises fusionnent aujourd'hui bureaux professionnels et environnement personnel, la sécurité de l'impression ne doit plus être un point faible. Le scénario selon lequel une imprimante serait utilisée pour infecter l'ensemble du réseau d'une entreprise est une réelle possibilité. 45 % des décisionnaires IT déclarent avoir constaté l'utilisation d'imprimantes compromises comme point d'attaque au cours de l'année passée. Le moment est venu pour les entreprises de prendre conscience de ce problème et de se protéger contre les attaques qui visent les imprimantes. »

S'ADAPTER À CETTE NOUVELLE NORMALITÉ

RÉSUMÉ DES RÉSULTATS DU RAPPORT HP WOLF SECURITY :

- La pandémie a entraîné un changement permanent : l'adoption du télétravail à domicile pour davantage d'employés.
- L'environnement de télétravail à domicile est très différent en termes de sécurité car les employés prennent plus de risques qu'au bureau, par exemple en utilisant des appareils non protégés, en partageant ces appareils avec leurs proches et amis ou en utilisant ces appareils de travail pour un usage personnel.
- Les personnes mal intentionnées ont repéré cette vulnérabilité et ciblent désormais les télétravailleurs via des campagnes de malwares dédiées s'appuyant sur le piratage psychologique. Ces dernières compliquent le travail des équipes IT déjà sur-sollicitées, tout en rendant invisibles de nombreux risques liés au télétravail.
- Cette situation a mis en lumière les limites de l'approche actuelle de la sécurité des terminaux, basée sur des politiques de confiance héritées de l'ère de la sécurité périmétrique. Lorsqu'un problème apparaît dans un tel contexte, il est souvent impossible de le voir jusqu'à ce que des dégâts majeurs soient constatés.

La question clé subsiste donc : dans un monde où chacune et chacun peut travailler depuis n'importe où, comment pouvons-nous développer les équipes hybrides de demain sans exposer les entreprises à plus de cybermenaces ? Un(e) employé(e) qui prête son ordinateur portable de travail à son enfant pour télécharger des jeux peut être considéré(e) comme insouciant(e) mais un tel comportement est également compréhensible, car beaucoup tentent aujourd'hui de trouver un équilibre entre travail et vie personnelle, et les données recueillies indiquent clairement que ces personnes sont bien loin d'être seules. Ces enjeux ne reposent pas sur un moment unique dans le temps. Si la pandémie a encouragé les entreprises à adopter de nouvelles approches et accéléré l'adoption du télétravail, elle a aussi certainement transformé à tout jamais la manière dont les gens travaillent. Les entreprises doivent rapidement analyser la manière dont elles gèrent ces risques dans ce nouvel environnement de travail, et optimiser simultanément la mobilité et la sécurité de leurs employés.

CONCLUSIONS LIÉES À HP WOLF SECURITY

UNE NOUVELLE APPROCHE EST NÉCESSAIRE

Les cybercriminels sont aujourd'hui plus intelligents, organisés et déterminés que jamais. La transformation numérique et des données élargit la surface d'attaque. Malgré leurs efforts, les équipes IT et de sécurité sur-sollicitées ont des difficultés à suivre le rythme. Dans ce contexte, la sécurité des terminaux est une première ligne de défense plus vitale que jamais. Si un(e) employé(e) peut être persuadé(e) de contourner un outil de contrôle, d'ignorer un avertissement ou tout simplement d'être négligent(e), ces outils de contrôle pourraient tout aussi bien ne pas exister. Quand les mesures de sécurité défaillent, elles le font souvent de manière significative et permettent aux personnes mal intentionnées de pénétrer dans les systèmes, d'en extraire des données, d'espionner et de perturber leur fonctionnement à leur gré. Ce problème n'est pas nouveau, mais l'adoption globale du télétravail lui a conféré une toute nouvelle dimension.

La solution radicale à ce problème est d'appliquer l'équivalent technologique d'un confinement. L'accès est restreint, des couches d'authentification sont ajoutées de manière non coordonnée et l'utilisation des appareils est limitée par des politiques. Dans le cadre du télétravail, cette situation entraîne rapidement des problèmes, nuit à la productivité des employés et renforce l'idée que la sécurité est un obstacle.

L'alternative, souvent défendue dans le secteur, est de « détecter pour protéger » en recherchant des signatures et codes connus pour être nuisibles. Mais l'essor des malwares polymorphes et auto-générés, par exemple des malwares générés par des machines, entrave de telles approches. La nouvelle génération d'outils de détection tente de résoudre ce problème en tirant parti de l'apprentissage automatique pour repérer les mutations possibles, mais les développeurs de malwares ont également accès à ces outils. Ils peuvent tester automatiquement leur code et le modifier jusqu'à ce qu'il ne soit plus détecté, les confortant ainsi dans leur idée qu'il restera impossible à repérer. Et certaines attaques parviennent toujours à passer à travers les mailles du filet.

APPLICATION DE PRINCIPES DE CONFIANCE ZÉRO (ZERO TRUST)

Trouver un nouvel équilibre entre les besoins de sécurité et les besoins des employés nécessite d'adopter une toute nouvelle approche de la sécurité des terminaux et du télétravail à domicile. En se basant sur une approche de confiance zéro (Zero Trust), qui affirme qu'aucune confiance implicite ne devrait être accordée à quelque élément que ce soit, l'accès aux ressources devrait être évalué en fonction du contexte – par exemple, en fonction de l'utilisateur, de l'appareil, de l'emplacement et de la stratégie de sécurité. De manière cruciale, cette approche s'applique non seulement aux appareils mais aussi aux différents éléments composant ces appareils eux-mêmes, y compris le microprogramme, la sécurité des applications, l'intégrité du système d'exploitation et le compte ou utilisateur accédant aux données.

Un monde numérique décentralisé ne signifie pas nécessairement un monde plus vulnérable. Notre cybermonde évolue constamment ; la cybersécurité doit suivre. La technologie du futur proche sera délibérément sécurisée et suffisamment intelligente pour non seulement détecter les menaces, mais aussi les contrôler et atténuer leur impact, ainsi que récupérer rapidement en cas de violation de données. Aider nos clients à évoluer de manière sûre dans cet écosystème numérique dynamique est notre mission chez HP.

HP WOLF SECURITY – UNE SÉCURITÉ NOUVELLE GÉNÉRATION POUR LA SÉCURITÉ DES TERMINAUX[1]

Avec cette mission en tête, HP présente HP Wolf Security – notre nouveau portefeuille de PC et imprimantes dotés de logiciels de sécurité des terminaux, directement intégré au matériel – afin d'aider nos clients à évoluer dans ce paysage complexe et se défendre contre le large éventail de nouvelles attaques et nouveaux risques liés à notre nouveau mode de vie de plus en plus décentralisé. La plateforme HP Wolf Security s'appuie sur plus de 20 ans de recherches et d'innovations en matière de sécurité pour offrir un portefeuille de produits uniformisé aux clients en quête d'une protection pour terminaux dans l'optique d'une politique cyber résiliente.

Basée sur des principes de confiance zéro (Zero Trust), la solution HP Wolf Security offre une défense et une protection de pointe, assure une confidentialité et est dotée d'un système intelligent, recueillant des données sur les terminaux pour aider à protéger l'entreprise tout entière contre les menaces.

HP Wolf Security aide les entreprises à se défendre contre les menaces connues et inconnues, et même contre les vulnérabilités « zero-day ». Combinant des logiciels et fonctionnalités de sécurité renforcées grâce au matériel et des services de sécurité des terminaux de pointe dans le secteur, HP Wolf Security permet une sécurité multicouche et une intégration fluide aux autres solutions de sécurité. Ainsi, les clients bénéficient d'une protection intégrée robuste à tous les niveaux, du matériel au cloud et du BIOS au navigateur.

Pendant trop longtemps, les terminaux ont été considérés comme des victimes devancées par des ennemis pouvant être combattus uniquement grâce à une détection des activités problématiques sur le réseau. Cette vision était toujours optimiste. Une fois qu'une menace dépasse les frontières des terminaux, le danger qu'elle représente est très fortement augmenté. L'endroit approprié pour éradiquer les menaces est l'endroit même où elles apparaissent, au sein de la couche logicielle compromise. Aucune attaque ne devrait jamais pouvoir compromettre un terminal et poursuivre son chemin en toute impunité.

HP Wolf Security aide à protéger les entreprises contre les menaces liées au télétravail et continuera à implémenter de nouvelles fonctionnalités de sécurité afin d'aider les utilisateurs à se protéger contre l'évolution des menaces. Certains exemples actuels incluent :

- **Protection des applications clés contre les cybermenaces** : la solution HP Wolf Enterprise Security inclut la fonctionnalité Sure Access Enterprise[2], qui applique la technologie d'isolation unique de HP afin de garantir la protection totale des applications essentielles contre tout malware présent sur le PC d'un utilisateur. HP Sure Access crée des micro-machines virtuelles renforcées grâce au matériel qui permettent de protéger les applications clés – formant ainsi une couche de sécurité virtuelle entre l'application et le PC utilisé. L'application et les données sont isolées de manière sécurisée du système d'exploitation et de toute personne mal intentionnée qui aurait pu y accéder.
- **Élimination des risques liés aux malwares via la maîtrise des menaces et l'isolation** : la micro-virtualisation permise grâce au matériel isole de manière totale les menaces liées aux facteurs les plus couramment utilisés – e-mails, navigateurs et téléchargements – sans impact sur l'expérience utilisateur. Lorsqu'une tâche est finalisée, la micro-machine virtuelle – et toute menace contenue au sein de celle-ci – est supprimée, sans violation de données. Ainsi, même si un utilisateur clique sur un élément problématique, la personne mal intentionnée l'ayant créé ne peut accéder à aucune donnée et ne peut rien subtiliser.
- **Récupération rapide après une attaque à distance ciblant le microprogramme et réduction de la pression subie par le département IT** : souvent délaissés, les imprimantes et scanners et leur mauvaise utilisation représentent une menace de sécurité croissante. HP Wolf Security résout ce problème en permettant une visibilité et une gestion exhaustives de chaque couche logicielle des imprimantes, y compris la possibilité de modifier le microprogramme et la capacité d'auto-réparation au cas où ces appareils auraient été compromis par un malware. La fonctionnalité de sécurité instantanée applique également immédiatement la politique de sécurité de l'entreprise aux appareils lorsqu'ils sont ajoutés au réseau. HP Security Manager permet également d'appliquer plus de 200 paramètres de sécurité aux modèles d'appareils compatibles.
- **Utilisation de données télémétriques sur les menaces pour transformer une faiblesse traditionnelle – les terminaux – en source de collecte d'informations** : recueillez des données uniques sur les menaces en permettant aux attaques de se dérouler dans un environnement sécurisé et contrôlé, afin de vous aider à mieux comprendre les menaces visant votre entreprise. Utilisez les informations cloud et données recueillies via les terminaux pour améliorer la collecte de données sur les menaces, tout en profitant d'un aperçu plus global de la sécurité de votre entreprise en automatisant les alertes liées à vos appareils d'impression connectés au sein de votre système d'outils de gestion des événements et informations de sécurité (SIEM).

Tout cela rejoint l'objectif principal de HP : nous sommes là pour réduire les pressions subies par les équipes IT et en charge de la sécurité et les aider à affronter des cybermenaces sans précédent, et pour aider les utilisateurs et clients à continuer à travailler de manière sécurisée depuis chez eux ou à distance. Rendez-vous sur la page d'accueil HP Wolf Security pour en savoir plus.

MÉTHODOLOGIE

Les résultats présentés dans ce rapport proviennent de quatre sources de données distinctes :

01 Une enquête en ligne réalisée par YouGov auprès de 8 443 adultes vivant aux États-Unis, au Royaume-Uni, au Mexique, en Allemagne, en Australie, au Canada et au Japon, anciens employés de bureau et travaillant chez eux autant ou plus qu'avant la pandémie. Ces données ont été recueillies entre le 17 et le 25 mars 2021. Cette enquête a été effectuée en ligne.

02 Une enquête réalisée par Toluna auprès de 1 100 décisionnaires IT aux États-Unis, au Royaume-Uni, au Mexique, en Allemagne, en Australie, au Canada et au Japon. Les personnes interrogées travaillent dans des entreprises comptant 50 à 99 employés (25 %), 100 à 499 employés (26 %), 500 à 999 employés (26 %) et plus de 1 000 employés (24 %). Ces données ont été recueillies entre le 19 mars et le 6 avril 2021. Cette enquête a été effectuée en ligne.

03 Le rapport *The 2020 Cybersecurity Threat Landscape for Remote Workers as a Result of the COVID-19 Pandemic* (Les menaces de cybersécurité pour les télétravailleurs en 2020 suite à la pandémie de COVID-19) créé par KuppingerCole en mars 2021. Ce dernier fournit un contexte et une analyse liés à l'évolution de l'environnement de travail en 2020 en raison de la pandémie de COVID-19, et se penche sur les activités et habitudes des entreprises et employés dans le monde entier ainsi que sur les activités et tendances des personnes mal intentionnées liées aux vulnérabilités apparues à cause de ce nouveau contexte professionnel.

04 Des données sur les menaces capturées au sein de machines virtuelles de clients HP équipées de Sure Click, et des analyses effectuées par l'équipe de HP responsable des informations sur les menaces.

CLAUSES DE NON-RESPONSABILITÉ

[1] HP Security devient HP Wolf Security. Les fonctionnalités de sécurité varient selon les plateformes. Veuillez consulter les fiches techniques des produits pour plus de détails.

[2] HP Sure Access Enterprise requiert Windows 10 Pro ou Entreprise. Les services HP sont régis par les conditions générales de service HP applicables, qui sont remises au client ou lui sont indiquées lors de l'achat. Le client peut disposer de droits supplémentaires accordés par les lois locales, qui ne peuvent en aucun cas être affectés par les conditions générales applicables au service HP ou la garantie limitée accompagnant le produit HP. Pour connaître la configuration système requise, rendez-vous sur www.hpdaas.com/requirements.

HP WOLF SECURITY