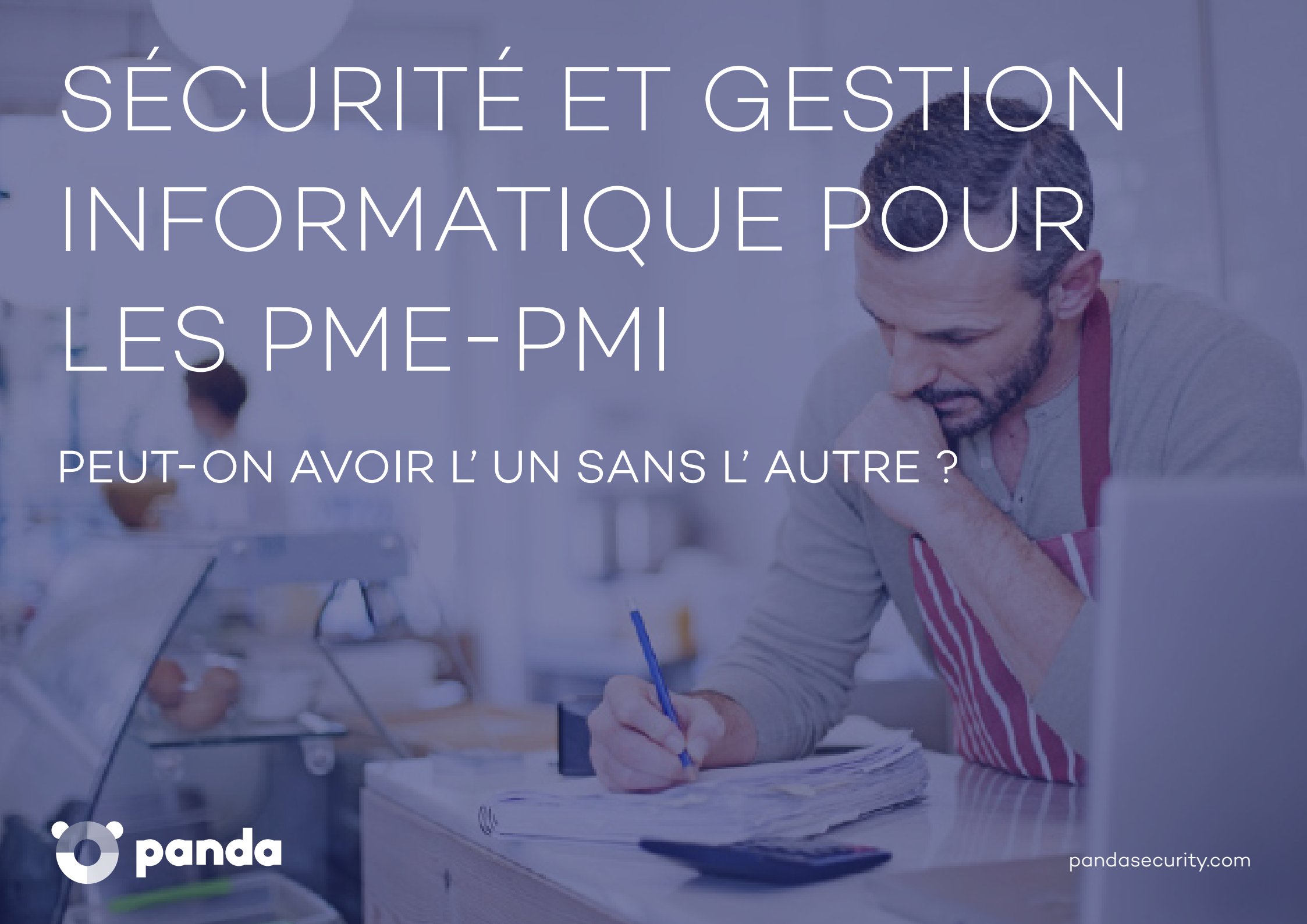
SÉCURITÉ ET GESTION INFORMATIQUE POUR LES PME-PMI

PEUT-ON AVOIR L' UN SANS L' AUTRE ?



panda

pandasecurity.com

Les logiciels malveillants recherchent maintenant les gains économiques plutôt que les nuisances gratuites.

La nature de la sécurité est en train d'évoluer pour s'adapter à un panorama de menaces lui-même en constante évolution. Alors que la plupart des secteurs subissent une transformation technologique du fait du Cloud, de la mobilité et, dans une certaine mesure, du Big Data, la sécurité informatique n'est pas en reste et doit aussi faire face à une profonde mutation.

Les auteurs de logiciels malveillants sont depuis un certain temps motivés par les gains financiers plutôt que par leur seule recherche de notoriété comme c'était le cas lorsque les virus **I Love You* et Anna Kournikova captaient l'attention du public et des médias il y a de nombreuses années.**

Comme dans tous les autres secteurs, lorsque l'opportunité de gain commence à faire son apparition, des compétences se manifestent pour en profiter.

Le but est aujourd'hui clairement économique et plus un logiciel malveillant peut demeurer longtemps sur des systèmes à l'abri des regards, plus cela peut rapporter à son propriétaire.

On estime que le virus I love you a affecté 45 millions de PC et provoqué entre 5,5 et 8,7 milliards de dollars de dommages dans le monde. Le coût de l'élimination de ce ver aurait été de 15 milliards de dollars.

Il n'a toutefois procuré aucun gain économique à ses développeurs (Wikipédia)

Les investissements en logiciels malveillants atteignent des sommets

Cet afflux de capitaux dans le développement de logiciels malveillants bat tous les records de ce domaine ; en 2014, le nombre de logiciels malveillants créés a représenté 34 % de tous les logiciels malveillants détectés par le PandaLabs depuis sa création avec 205 000 nouvelles moutures produites en moyenne CHAQUE JOUR.

En tête de liste des menaces, nous trouvons toujours les chevaux de Troie, ce type de logiciel malveillant conçu pour exploiter les vulnérabilités des systèmes et des applications, qui sont elles-mêmes un autre aspect du problème global de la protection.

220 millions

NOMBRE TOTAL D'ÉCHANTILLONS DE LOGICIELS MALVEILLANTS IDENTIFIÉS PAR LE PANDALABS

30,42 %

ORDINATEURS INFECTÉS DANS LE MONDE ENTIER

3 500 CHAQUE HEURE

205 000 PAR JOUR

2014 **75** MILLIONS

28,96 %	USA
30,90 %	Espagne
34,12 %	Brésil
25,68 %	France
22,14 %	Angleterre
19,98 %	Suède
22,68 %	Allemagne
38,80 %	Russie
49,05 %	Chine
24,84 %	Japon

Source : Rapport annuel PandaLabs 2014

Les environnements mobiles actuels, hétérogènes et disséminés, compliquent la gestion et ajoutent des failles de sécurité.

À mesure que les dépenses et la dépendance des entreprises aux matériels et aux logiciels augmentent, les systèmes informatiques deviennent de plus en plus répartis, hétérogènes et difficiles à gérer. Du simple point de vue du volume, les services informatiques doivent maintenant relever le défi de la gestion de plusieurs sites, plusieurs systèmes d'exploitation et plusieurs appareils par utilisateur.
Chaque nouvel appareil accroît l'efficacité de l'entreprise mais crée une vulnérabilité supplémentaire.

Dans le domaine de la mobilité, nous voyons clairement que ce problème est encore plus aigu pour les PME, comme le cabinet d'analyse Gartner l'a mentionné dans un récent rapport* ; les PME doivent en effet relever pratiquement les mêmes défis que les entreprises de plus grande taille pour assurer la maîtrise et la sécurité de leurs appareils mobiles.

Toute cette complexité sollicite les équipes techniques au-delà des limites et crée des maillons faibles dans la sécurité globale du périmetre.

Par exemple, un des problèmes de sécurité liés à la protection de ce nouveau maillage technologique réside dans la croyance que certains appareils, sous MAC ou Linux notamment, ne sont pas vulnérables et ne nécéssitent pas de protection.

« La plus grande vulnérabilité du Macintosh réside dans la croyance au sein de ses utilisateurs que le système d'exploitation d'Apple est supérieur et que cela le rend invulnérable aux logiciels malveillants »**. Cette idée fausse laisse la porte ouverte aux logiciels malveillants (y compris les logiciels malveillants Windows) en leur permettant de profiter de ces maillons plus faibles pour pénétrer sans résistance dans le réseau.

*Gartner_Mars 2014

Les six points clés de la gestion des appareils mobiles pour les PME.

** Livre blanc_Mai 2014
Devrais-je me soucier des virus sur mon MAC ?

• Les dépenses liées à la mobilité des PME aux États-Unis et au Canada devraient atteindre 71,5 milliards de dollars d'ici 2018, selon AMI. On prévoit, par exemple, un TCAM de 21 % aux États-Unis et au Canada rien que pour les tablettes.

http://www.ami-partners.com/index.

• Gartner prévoit que d'ici 2017, 50 % des employeurs demanderont à leurs collaborateurs d'utiliser leurs appareils personnels au travail

http://www.gartner.com/newsroom/id/2466615

Un premier pas dans la bonne direction : le Cloud, d'un choix d'avant-garde à une nécessité industrielle.

Avec des créations de logiciels malveillants qui battent tous les records, les fournisseurs de sécurité ne peuvent plus se fier uniquement à des solutions locales basées sur des fichiers de signatures pour protéger les systèmes informatiques de leurs clients. En plus de leur capacité de détection réduite, de telles solutions pénalisent les réseaux de façon de plus en plus marquée à mesure que le nombre de logiciels malveillants augmente.

Les fournisseurs de sécurité se tournent maintenant vers le Cloud et la puissance de traitement exceptionnelle du Big Data pour répondre à une menace d'envergure, toujours plus présente, en transférant la charge de travail du réseau et de l'appareil vers le Cloud. Cette mutation a permis à certains fournisseurs de sécurité de prendre pleinement pied dans le nouveau paysage des menaces informatiques, tout en permettant aux entreprises de se concentrer sur leurs activités et non sur la gestion de la sécurité. Il s'agit là d'un grand pas dans la bonne direction mais, comme nous l'avons mentionné, cela ne traite qu'une partie du problème.

Les vulnérabilités des systèmes et des logiciels sont maintenant à la base de la grande majorité des infections, et les directeurs informatiques avisés savent que se concentrer uniquement sur les meilleurs antivirus et les meilleurs firewalls, même basés dans le Cloud, ne suffit plus à traiter de façon appropriée un problème qui ne fait que croître.

Plus de 90 % des infections sont causées par des vulnérabilités non corrigées, habituellement dans des logiciels tiers tels que Java, Adobe, Flash, etc.

PandaLabs 2014

La majorité des solutions locales reposent sur des fichiers de signatures qui se mettent habituellement à jour une fois toutes les 24 heures, parfois moins, mais cette fréquence est clairement insuffisante face aux 205 000 nouveaux logiciels malveillants qui apparaissent chaque jour sur Internet, selon le rapport 2014 du PandaLabs.

Une solution basée sur le Cloud garantit de rester constamment à jour, en réduisant la charge de gestion et en n'imposant pas de matériel ou de logiciel supplémentaire dans le réseau.

La convergence de la sécurité et de la gestion.

Les vulnérabilités des systèmes et des applications devenant de plus en plus critiques, il est logique que **la sécurité et la gestion des appareils** convergent. La sécurité dépasse désormais l'approche traditionnelle des antivirus et des firewalls, pour englober un cadre beaucoup plus large qui va de la visibilité à la mise en application de stratégies. Pour être tout à fait complet, ce nouveau cadre doit aussi prendre en compte la résolution des problèmes, et il doit pouvoir s'appliquer à tous les systèmes informatiques sans exception.

Jusqu'à récemment (durant le règne du PC), avec les réseaux locaux équipés en grande majorité de stations de travail et de serveurs Windows, il était possible de gérer la plupart des aspects des mises à jour des systèmes et des applications, même si cela prenait beaucoup de temps. Aujourd'hui, dans l'ère post-PC, l'exception est devenue la règle mais le défi reste le même ; pour réduire la menace de sécurité globale, les responsables informatiques DOIVENT pouvoir gérer chaque appareil quel que soit son emplacement. Concrètement, ils doivent garantir la visibilité permanente des terminaux et s'assurer que les appareils sont à jour, équipés de tous les correctifs et optimisés. En cas de problème, des mécanismes doivent permettre de réagir rapidement et efficacement.

Malheureusement, dans les entreprises actuelles, la visibilité permanente sur les environnements hétérogènes répartis est encore loin d'être la norme.

Microsoft estime que 40 % seulement des entreprises disposent d'une véritable gestion crédible des appareils.

Réduction de la fragmentation et de la complexité.

Dispersion

Les environnements fragmentés équipés de nombreux types d'appareils différents peuvent conduire à la mise en œuvre de correctifs rapides, de solutions fragmentées ; une solution pour les mises à jour logicielles, une autre pour la sécurité, une autre encore pour l'assistance à distance, pour le MDM... etc. Pour pouvoir maîtriser le problème et parvenir à une meilleure efficacité avec les mêmes équipes, la solution doit être centralisée. Tous les appareils et toutes les tâches accessibles à partir d'une solution unique pour toute l'équipe informatique, depuis n'importe quel lieu et à tout moment.

Complexité

Elle est inhérente au problème, différents appareils par utilisateur, différents sites, le BYOD. Toutefois, répondre au problème avec des solutions fragmentées ne fait qu'engendrer un cercle vicieux dans lequel la complexité augmente à chaque solution supplémentaire mise en œuvre. Votre choix doit se porter sur une solution à même de vous procurer rapidement de la valeur, facile à mettre en œuvre et à gérer, ne nécessitant pratiquement aucun effort d'apprentissage, une solution qui vous simplifie les systèmes informatiques complexes d'aujourd'hui.

En résumé

Motivés par des gains économiques, les logiciels malveillants connaissent une croissance exponentielle. Les PME doivent relever le défi de la gestion de systèmes informatiques plus hétérogènes, plus complexes et plus répartis, et cela ne fait qu'amplifier le problème de la sécurité en créant des failles supplémentaires et en sollicitant les ressources humaines existantes au-delà des limites.

Le Cloud, la mobilité et le Big Data font partie intégrante non seulement de cette nouvelle réalité informatique mais aussi de sa protection et de sa gestion. La gestion des appareils converge maintenant avec la sécurité, et les entreprises peuvent aborder la sécurité avec un point de vue plus large tout en bénéficiant de gains de performances conséquents. Pour être adoptée et exploitée par les PME, cette convergence doit être centralisée, complète et NON complexe.

La question n'est PAS de savoir si vous avez besoin de gérer et de sécuriser chaque appareil, mais comment le faire AU MIEUX en traitant les problèmes sous-jacents comme la fragmentation et la complexité des outils.

Panda Cloud Fusion

Panda Cloud Fusion vise à simplifier et à centraliser la sécurité, la gestion et le support par le Cloud. Panda Security propose une approche complète de la gestion des systèmes dans laquelle chaque appareil compte ; qu'il s'agisse d'un poste Windows XP, d'un serveur Linux, d'un MacBook ou d'une tablette / d'un smartphone, qu'il soit connecté au réseau ou non, vous pouvez gérer, sécuriser et assurer le support de tous les appareils à partir d'une console centralisée.

Comme Gartner l'a mentionné en janvier 2014 dans son Carré magique EPP : « Panda est [aussi] le premier fournisseur de protection du poste client à prendre totalement en charge la prestation de services de sécurité par le Cloud. » En le classant comme visionnaire pour la protection des postes clients, Gartner souligne la fonction de protection de Panda et sa capacité à « intercepter les menaces les plus récentes » grâce à ses détections de type comportemental et à sa connaissance basée sur le Cloud, l'Intelligence Collective.

Dans le même rapport, Gartner mentionne les points forts de la « solution de gestion de système de poste client ajoutée récemment, qui inclut des capacités d'audit, de configuration, de distribution des correctifs et des logiciels, ainsi qu'une commande à distance ».

L'audit centralisé permet aux administrateurs informatiques d'avoir une visibilité permanente de tous leurs systèmes informatiques, mobiles et smartphones inclus, à partir d'une console unique. Les fonctions intégrées de gestion de correctifs et de distribution de logiciels garantissent que les systèmes seront à jour et optimisés, ce qui réduira la menace d'attaques virales via des vulnérabilités.

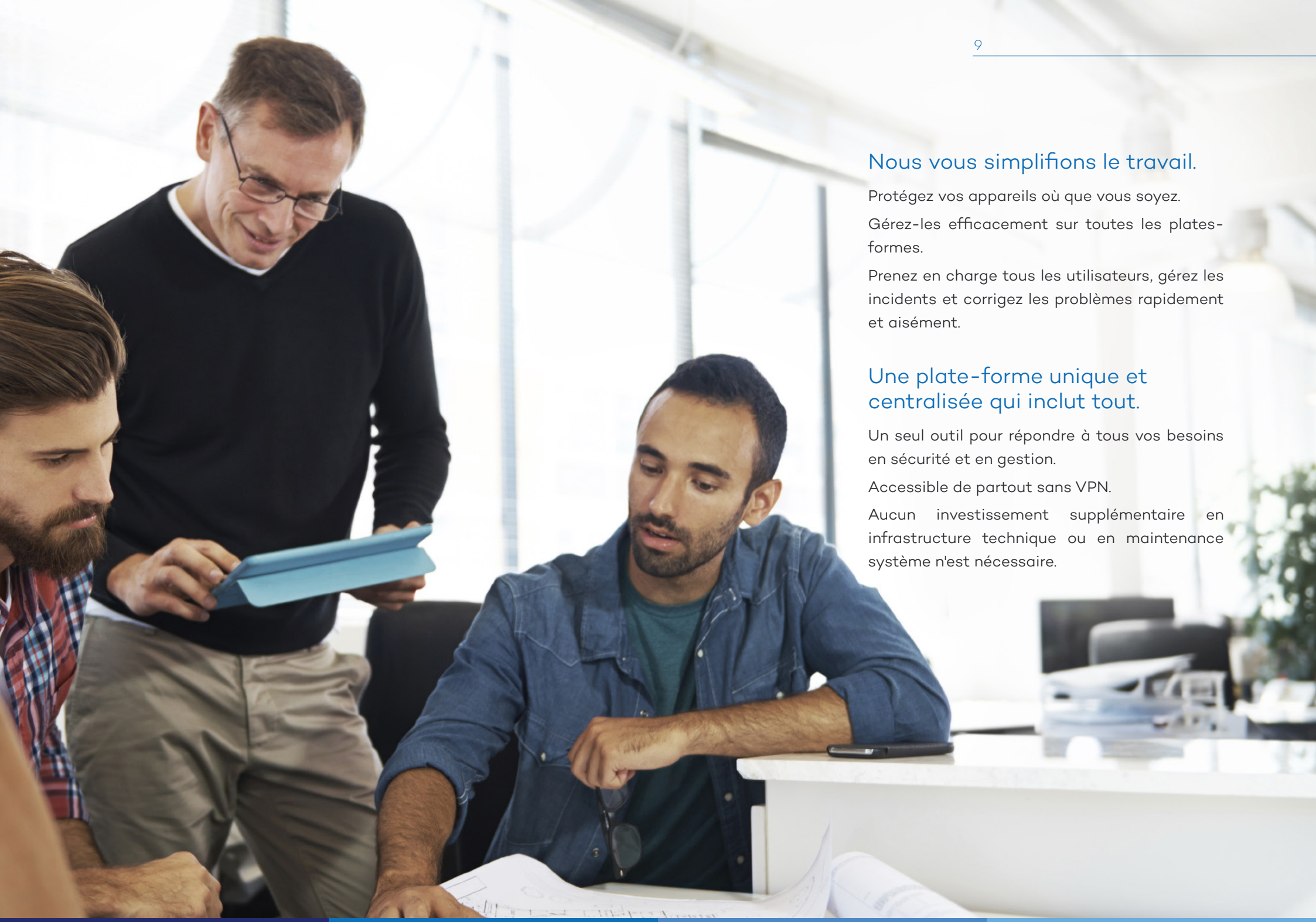
Le support non intrusif à distance complète l'offre en permettant aux techniciens d'effectuer des diagnostics complets d'incidents et de mettre en œuvre des solutions en arrière-plan pendant que les utilisateurs finaux continuent d'utiliser leurs systèmes.

En plus d'optimiser et de sécuriser tous vos appareils, Panda Cloud Fusion permet aux professionnels d'être plus efficaces dans l'automatisation de la plupart des tâches informatiques courantes, via un ensemble de fonctionnalités faciles à utiliser. L'automatisation, comme la surveillance des systèmes avec des réponses prédéfinies et le suivi des incidents via des tickets de support, permet aux professionnels du service informatique de se concentrer sur des projets à plus grande valeur ajoutée tout en garantissant une qualité de service constante.

Pour en savoir plus sur Panda Cloud Solution

Essayez-le pendant 30 jours

Téléchargez ici



Nous vous simplifions le travail.

Protégez vos appareils où que vous soyez.

Gérez-les efficacement sur toutes les plates-formes.

Prenez en charge tous les utilisateurs, gérez les incidents et corrigez les problèmes rapidement et aisément.

Une plate-forme unique et centralisée qui inclut tout.

Un seul outil pour répondre à tous vos besoins en sécurité et en gestion.

Accessible de partout sans VPN.

Aucun investissement supplémentaire en infrastructure technique ou en maintenance système n'est nécessaire.


panda