Kiteworks

Supprimez les risques associés aux déplacements de vos cadres dirigeants

5 bonnes pratiques pour sécuriser les communications de contenu sensibles de vos cadres dirigeants

Sommaire

Les chefs d'entreprise et cadres supérieurs envoient et reçoivent chaque jour des informations critiques pour l'entreprise depuis des emplacements à risque, en utilisant les appareils les moins sécurisés : leurs téléphones mobiles et leurs tablettes. Ils dépendent de ces appareils pour rester productifs malgré un horaire de voyage chargé, quand ils partent rencontrer des clients, des investisseurs ou des filiales.

Après tout, ils ne peuvent pas stopper toutes leurs activités pendant qu'ils voyagent, ou même lorsqu'ils sont coincés dans une série de réunions. Chaque jour, leurs équipes leur envoient des documents, des présentations, des demandes de validation d'achat et des rapports sur l'avancement des projets. Les dirigeants sont amenés à travailler avec le conseil d'administration et les avocats, à revoir la dernière version d'un contrat, et ce depuis un aéroport, un hôtel ou un couloir pendant des périodes de temps libre.

Néanmoins, cette recherche de productivité s'accompagne d'un risque d'exposition involontaire d'informations confidentielles (résultats financiers préliminaires, fusions et acquisitions, négociations, poursuites judiciaires ou secrets commerciaux) avec des conséquences susceptibles de nuire à l'entreprise. Réduisez les risques en adoptant cinq bonnes pratiques pour optimiser la productivité mobile de vos cadres dirigeants tout en protégeant les secrets de votre entreprise.

Bonne pratique #1 :

01 Veiller à la productivité et la sécurité des cadres en déplacement

Garantir une messagerie mobile simple et sécurisée

Les dirigeants d'entreprise utilisent leur messagerie mobile toute la journée pour partager des rapports financiers avec les membres du conseil d'administration, solliciter des conseils juridiques confidentiels auprès de leurs avocats, ou pour d'autres types de communications confidentielles. Mais s'ils transfèrent des e-mails et des pièces jointes en utilisant des outils de messagerie standards, ils s'exposent à l'analyse des opérateurs téléphoniques, des gouvernements et des pirates. Et quand le pire se produit, ils n'ont aucune traçabilité pour prouver qui avait accès à quels fichiers. Enfin, les messages reçus importants sont noyés dans les spams, ce qui retarde leurs réponses.

Évitez ce scénario en ajoutant une couche de protection supplémentaire à votre messagerie d'entreprise pour vos cadres. Facilitez son utilisation en proposant un système très simple à utiliser et qui offre un accès à distance sécurisé aux fichiers et répertoires du siège. Chiffrez tous les fichiers et messages en transit, ainsi que les fichiers hors ligne stockés sur l'appareil. Réduisez les spams en filtrant les expéditeurs inconnus. Et assurez-vous que vos cadres ne ratent aucune opportunité : une notification instantanée leur est envoyée lorsque le destinataire télécharge un document ou répond à un message.

Pour compléter, sécurisez le contenu côté destinataire, quel que soit le degré d'insécurité du système de messagerie de l'entreprise. Donnez à ces interlocuteurs externes un moyen simple et sécurisé de consulter les messages et de télécharger les pièces jointes, et chiffrez automatiquement leurs réponses sans avoir à installer de logiciel.

Bonne pratique #2 :

02 Aidez vos équipes à préparer et à épauler les cadres en déplacement

Envoyez du contenu en toute sécurité sur les appareils mobiles

Les communications internes sont tout aussi importantes que les échanges en externe. Lorsqu'un dirigeant se déplace pour enchaîner les réunions, son équipe doit préparer les ordres du jour, les dossiers de briefing et les supports de présentation. Ses collaborateurs pourront les transférer automatiquement dans les dossiers correspondants, de manière à ce qu'ils se trouvent déjà dans son appareil lorsqu'il ou elle aura le temps de les consulter et d'y répondre. Permettez à vos cadres dirigeants de pouvoir les ouvrir hors ligne ; un vol international peut être propice à la révision et à l'annotation d'une proposition complexe ou d'un contrat PDF.

Les communications internes sont tout aussi importantes que les échanges en externe.

Bonne pratique #3 :

03 Numériser et gouverner les communications du conseil d’administration

Mettre en place des dossiers partagés sécurisés

Vos plus grands risques de partage d’informations se produisent souvent avec des personnes étrangères à votre entreprise, comme les membres de votre conseil d’administration, vos avocats et banquiers, les sociétés d’investissement privées et les cabinets de conseil en fusions et acquisitions. Presque tout ce que vous partagez est susceptible d’arriver à l’oreille de vos concurrents et d’enfreindre les lois sur la divulgation financière. Et beaucoup de ces externes, comme vos cadres, consultent des informations en déplacement à l’aide de téléphones mobiles et de tablettes.

Conservez ces données qui évoluent constamment en les organisant soigneusement à l’aide de dossiers partagés. Configurez les autorisations de chaque dossier de sorte que seules les entités ayant besoin de savoir puissent les consulter, et que seules les personnes ayant besoin de les modifier puissent le faire. Et avec des informations aussi sensibles, veillez à mettre en place une traçabilité inviolable et des politiques d’expiration automatique.

Ajoutez un outil collaboratif pour les commissions externes qui travaillent ensemble sur des projets, tels que des contrats, des acquisitions ou des transactions financières. Proposez une version simple et fluide des applications Microsoft Word, Excel et PowerPoint, avec annotation et signature de PDF, en sauvegardant automatiquement les modifications dans le dossier partagé sécurisé. Que le destinataire externe passe par un navigateur ou une application mobile, envoyez des notifications, surveillez toutes les versions du fichier et conservez la traçabilité.

Bonne pratique #4 :

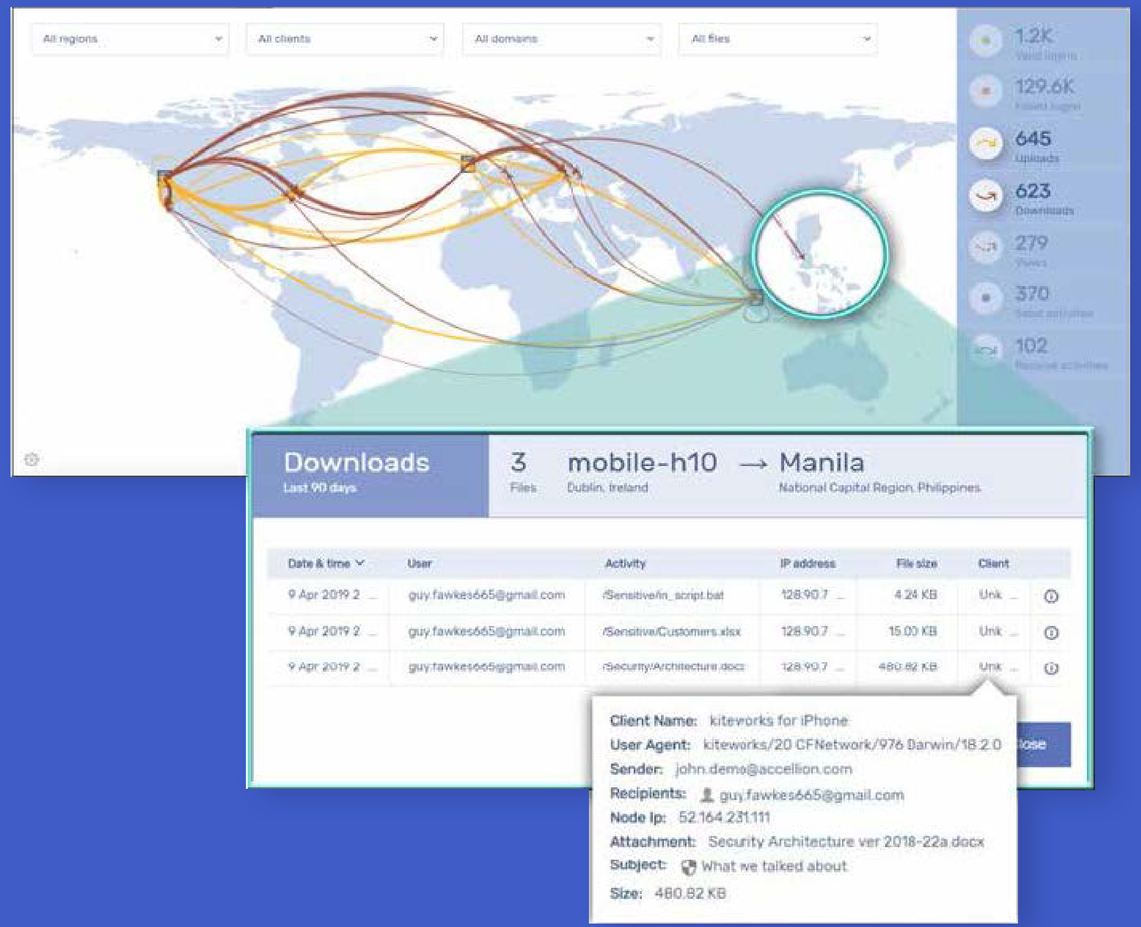
04 Sécurisez votre contenu mobile

Protégez intégralement vos fichiers sur n’importe quel appareil mobile

Aujourd’hui, vos cadres utilisent peut-être des partages de fichiers dans le cloud public et des e-mails non-chiffrés pour communiquer avec leurs collaborateurs et des personnes externes. Mais les fournisseurs de cloud public pour ces outils ont la capacité d’analyser les métadonnées de vos transferts de données, ce qui augmente les risques. Et lorsqu’ils reçoivent une assignation à comparaître, ils ont la capacité et l’obligation de remettre vos données confidentielles sans mandat.

Limitez les risques de la messagerie mobile et des dossiers partagés grâce à une infrastructure de sécurité et de gouvernance optimale. Implémentez le service sur un cluster de serveurs durci et évolutif, en chiffrant les informations avec des clés contrôlées par le service informatique lorsqu’elles sont en transit et lorsqu’elles sont stockées sur un appareil ou un serveur. Contrôlez qui a accès à vos données en déployant ce service à l’aide d’une infrastructure sur site, FedRAMP ou en cloud privé. Puisque les utilisateurs externes échappent à votre contrôle, renforcez l’application pour qu’elle s’exécute en toute sécurité sur leurs appareils personnels.

Donnez à l’administrateur les moyens de contrôler les politiques utilisateurs, de surveiller les utilisateurs d’appareils mobiles, d’établir une liste blanche des applications d’aide telles que Microsoft Word et d’intégrer des fonctions de sécurité telles que LDAP/AD et MDM. Enfin, éliminez le risque que représentent les données de l’entreprise sur un appareil introuvable ou volé en l’effaçant à distance, sans affecter le contenu personnel de l’utilisateur.



Bonne pratique #5 :

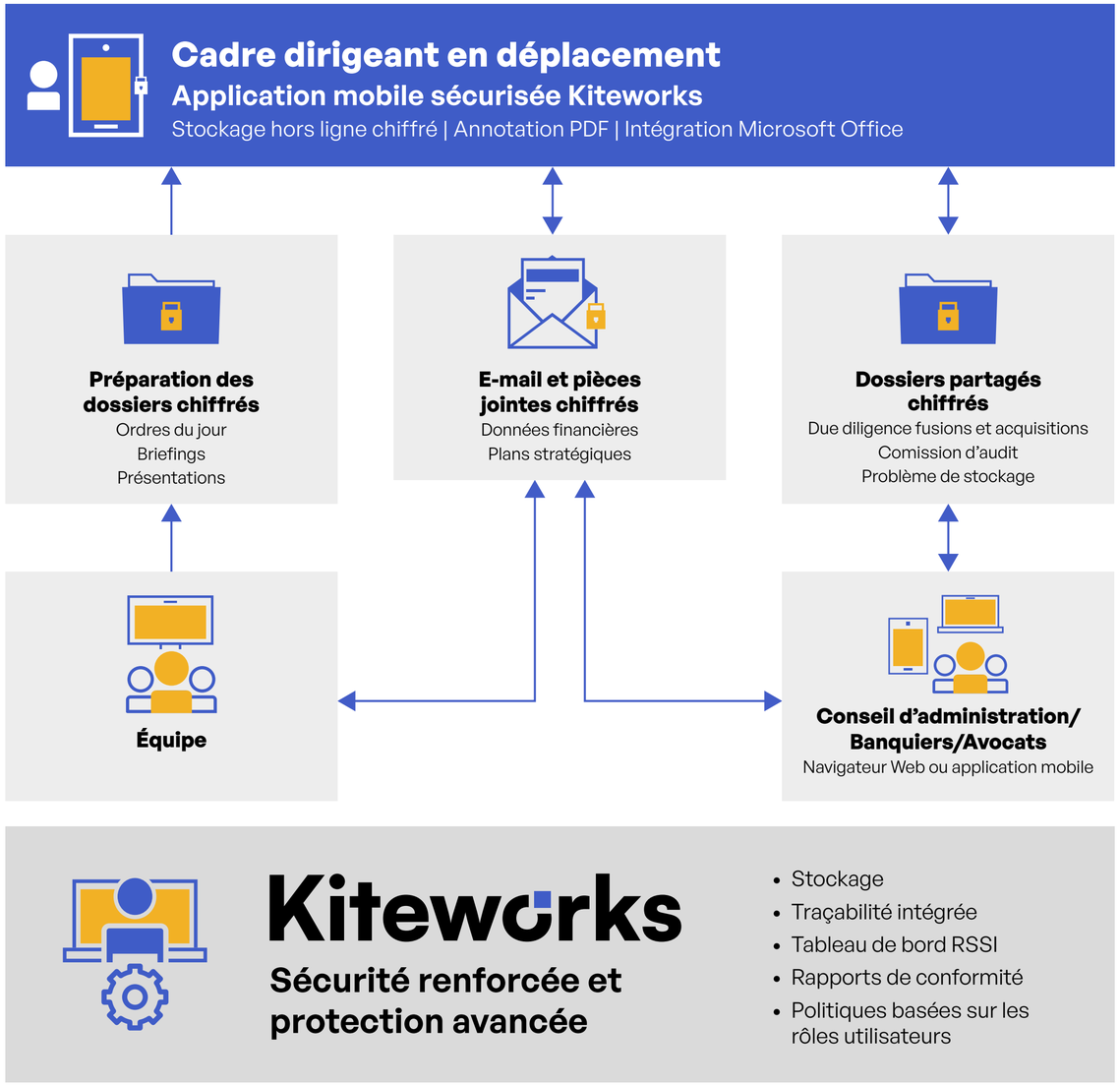
05 Prévenir les violations de données

Surveillez chaque transfert de fichier mobile

Pour vous défendre contre les menaces internes et externes de vos communications avec les cadres et les membres du conseil d'administration en déplacement, vous devez avoir connaissance de chaque fichier qui entre et sort de votre organisation via des appareils mobiles. Commencez par mettre en place une traçabilité globale de tous les transferts mobiles entre votre entreprise, ces voyageurs et les personnes externes. Une fois que vous disposez de toutes ces métadonnées, créez des affichages en temps réel clairs et complets qui répondent aux questions de sécurité les plus importantes concernant les informations qui entrent et sortent de l'entreprise. D'où viennent-elles ? Où vont-elles ? Qui les envoie ? À qui sont-elles transmises ? Sont-elles confidentielles ? La transaction est-elle normale ou représente-elle une menace ?

Réseau de contenu privé compatible avec Kiteworks

Prévenir les violations des téléphones et des violations de conformité



Kiteworks

www.kiteworks.com

Juillet 2022

 Kiteworks s'est donné une mission : aider les organisations à gérer efficacement les risques liés à l'envoi, à la réception, au partage et au stockage d'informations confidentielles. Avec la plateforme Kiteworks, nos clients disposent d'un réseau dédié à leurs contenus privés qui assure à la fois gouvernance, conformité et protection des données. La plateforme unifie, suit, contrôle et sécurise les partages des contenus sensibles, à l'intérieur de l'organisation mais aussi avec l'extérieur.
Ce faisant, elle améliore considérablement la gestion du risque et assure la conformité réglementaire de toutes les communications d'informations sensibles.