Forcepoint + Kiteworks

Une solution commune pour réduire de manière exhaustive les risques liés au contenu

Un réseau de contenu privé (PCN) Kiteworks associé à la solution zéro trust Content Disarm and Reconstruction (CDR) de Forcepoint, voici la toute première solution intégrée zéro trust pour la couche de contenu. Cette solution est la meilleure protection contre la divulgation d'informations sensibles à des tiers malveillants et contre les logiciels malveillants qui s'infiltrent dans le périmètre de l'entreprise.

Une solution unique. Le meilleur de la technologie mondiale. Spécialement conçu pour des environnements où les risques et les impacts peuvent être désastreux.

La multiplication des contenus et la fragmentation des systèmes de communication créent de nouvelles vulnérabilités potentielles que les organisations doivent corriger.

Nous connaissons tous le dicton « le contenu est roi ». Mais en cybersécurité, un fichier endommagé ou corrompu peut devenir un roi redoutable s'il n'est pas identifié comme menace. Un contenu peut avoir deux vulnérabilités majeures :

- **Vulnérabilité n°1 :** le caractère confidentiel des informations. Tous les contenus ne sont pas destinés au grand public ; une grande partie d'entre eux est réglementée, contrôlée, classifiée et restreinte. Les données confidentielles sont exposées aux attaques de pirates informatiques : elles représentent un risque cybernétique et financier important pour l'organisation qui les envoie, les reçoit ou les stocke.
- **Vulnérabilité n°2 :** les tiers non autorisés et programmes malicieux qui peuvent être installés dans le contenu lui-même. Lorsque le contenu est exploité, ces logiciels malveillants peuvent pénétrer dans les terminaux, les réseaux et les systèmes où sont stockées les données sensibles. L'organisation touchée peut subir une rançon, la corruption et la destruction de ses données, voire leur divulgation publique. Ce phénomène peut provoquer des dommages importants pour les clients, des poursuites, des actions en justice et une atteinte à la réputation.

Ces deux types de vulnérabilités présentent chacune un risque important, mais combinées, elles menacent de causer des dommages irréversibles à l'entreprise non protégée.

L'application des principes zéro trust à la couche de contenu atténue considérablement les risques

Fort heureusement, Kiteworks et Forcepoint se sont associés pour créer une solution unique et intégrée pour prévenir ces vulnérabilités : un réseau de contenu privé (PCN) Kiteworks doté d'une architecture zéro trust intégré à la solution zéro trust CDR de Forcepoint. Cette solution garantit la sécurité de la couche de contenu. Voici comment elle atténue les risques :

- **Toutes les entités sont suspectes par défaut, y compris le contenu lui-même.** Dans le cadre de la stratégie zéro trust, les entités sont non seulement les utilisateurs, mais aussi le contenu lui-même. Et le contenu peut comporter des menaces, connues ou non. Avec Forcepoint Zero Trust CDR, la philosophie « ne se fier à personne » s'étend à « ne se fier à aucun contenu », ce qui garantit que toutes les données non structurées (c'est-à-dire le contenu) sont supposées malveillantes. Le système extrait les données commerciales utiles des fichiers entrants, les compare aux structures appropriées pour le type de fichier, puis crée de nouveaux fichiers entièrement fonctionnels pour envoyer uniquement les informations sûres à leur destination presque instantanément.
- **Accès au *contenu* selon le principe du moindre privilège.** Le contrôle d'accès ne concerne pas seulement l'accès aux applications. Pour réduire véritablement les risques, ce principe doit s'appliquer aux actifs de contenu : tel contenu présente tel niveau de risque en fonction de sa sensibilité, de qui l'envoie, le reçoit, le consulte, le modifie ou le sauvegarde, à partir d'où et vers où. Le PCN de Kiteworks garantit que le principe du moindre privilège s'applique à chaque classe de contenu et à chaque contexte.
- **Surveillance permanente globale.** Vous ne pouvez pas surveiller ce que vous ne voyez pas ou ne pouvez pas contrôler. Avec un PCN compatible Kiteworks, tous les canaux de communication sont regroupés dans un seul système, ce qui permet d'unifier les contrôles et de centraliser les journaux d'audit, conformément au principe zéro trust. Et en ne conservant que le contenu fiable, le CDR zéro trust de Forcepoint vous permet de surveiller ce qui se cache derrière chaque actif, offrant ainsi une protection supplémentaire contre ce qui peut éventuellement s'y cacher.

Les flux de contenu sécurisé et conforme permettent de communiquer en toute sérénité

Pour permettre le CDR zéro trust, l'architecture de la solution doit prévoir deux types de flux de données sécurisés et conformes. Premièrement, les fichiers non approuvés doivent être livrés au serveur CDR. Deuxièmement, le contenu nettoyé qui en résulte doit être livré à sa destination prévue. Kiteworks intègre ces étapes de manière transparente dans ses flux de communication de contenu.

- **Diffusion de contenu non approuvé par le CDR zéro trust.** En tant que canal de communication de contenu externe, la plateforme Kiteworks met en quarantaine les fichiers de contenu entrants et non approuvés pour empêcher leur utilisation dans l'entreprise. Puis les envoie immédiatement au CDR pour traitement.
- **Livraison du contenu nettoyé à ses destinataires.** Lorsque le traitement CDR presque instantané est terminé, Kiteworks remplace le fichier mis en quarantaine par la version nettoyée. Les utilisateurs peuvent alors le télécharger en toute sécurité, l'enregistrer dans d'autres repositories, l'envoyer par e-mail ou l'automatiser pour le transférer via SFTP, transfert de fichiers géré (MFT) ou autres. Naturellement, Kiteworks peut sauvegarder la version originale mise en quarantaine pour l'analyser ultérieurement.

La problématique actuelle des risques ne concerne pas seulement la protection et le contrôle des terminaux, des applications et des réseaux, mais aussi des données elles-mêmes. La question est de savoir comment protéger votre organisation contre les risques financiers et de non-conformité dus aux vulnérabilités des contenus en votre possession. Heureusement, Kiteworks et Forcepoint sont bien conscients de ce risque. C'est pourquoi ils proposent à leurs clients la première solution intégrée du marché, qui étend le principe de sécurité zéro trust au niveau le plus important : la couche de contenu.

Pour en savoir plus sur les solutions zéro trust appliquées à la couche de contenu, rendez-vous sur kiteworks.com/contact-us/.

Kiteworks