Kiteworks

FICHE PRODUIT

L'appliance virtuelle durcie de Kiteworks possède plusieurs couches de sécurité pour réduire considérablement les risques et la gravité des attaques

L'appliance de communication de contenu privé la plus sécurisée du marché rassure les clients en réduisant le CVSS de 10 à 4 des vulnérabilités comme Log4Shell.

Kiteworks a fait de la sécurité une priorité pour son réseau de contenu privé, en intégrant tous les modules dans une appliance virtuelle durcie, qui réduit le score CVSS (Common Vulnerability Scoring System) de n'importe quelle vulnérabilité. Par conséquent, les vulnérabilités qui obtiennent des scores de gravité élevés, voire critiques, avec d'autres applications sont bien moins risquées pour les clients de Kiteworks. Cela se traduit par une meilleure protection des contenus privés et une protection avancée contre les menaces.

Atténuez les risques d'exploitabilité des failles

L'appliance virtuelle sécurisée de Kiteworks est conçue pour réduire le nombre de vulnérabilités potentielles de ses bibliothèques et accroître la difficulté de les exploiter.

- **Pare-feu réseau et WAF intégrés.** L'appliance virtuelle durcie n'ouvre que les ports nécessaires dans son pare-feu réseau intégré. Elle protège le contenu via des niveaux de services internes et des contrôles d'accès basés sur le principe du « moindre privilège ». Elle surveille et bloque en permanence les connexions malveillantes grâce à son IPS intégré, et les demandes Web indésirables via son WAF intégré.
- **Accès au moindre privilège zero-trust. Les administrateurs ne disposent que de quelques comptes utilisateurs privilégiés, chacun ayant des permissions restreintes et aucun accès au système d'exploitation. Pour avoir accès au système d'exploitation, en vue d'un diagnostic ou d'une réparation, un ingénieur support certifié et authentifié de Kiteworks reçoit un accès temporaire, entièrement connecté, via un protocole de sécurité en deux étapes qui nécessite l'accord préalable du client et de Kiteworks.**
- **Une surface d'attaque est réduite au minimum.** Kiteworks n'ajoute que les bibliothèques et les pilotes absolument nécessaires sur le système d'exploitation (OS) Linux nu et désactive les fonctions et les services non indispensables.

Réduire la gravité des incidents

Le réseau de contenu privé s'appuie également sur des mécanismes de défense intégrés et différentes couches de sécurité pour réduire l'impact sur la confidentialité, l'intégrité et la disponibilité:

- **Détection des anomalies grâce à l'IA.** L'IA intégrée détecte les transferts de données anormaux pour alerter rapidement les services de sécurité d'une fuite potentielle.
- **Détection avancée des intrusions et alertes.** Kiteworks surveille le comportement de tous les exécutables, des systèmes de fichiers et du trafic Web. Le logiciel applique des politiques strictes, envoie des alertes et interrompt les activités inhabituelles avant qu'un cyberattaquant ne puisse endommager ou exfiltrer du contenu sensible.

- **Blocage des menaces zero-day.** Kiteworks bloque l'accès direct d'un exploit au contenu, aux métadonnées, aux réseaux et à d'autres ressources, en exécutant des bibliothèques tierces dans un bac à sable au niveau de l'OS (plutôt que directement sur le système d'exploitation).

Résultat ? Log4Shell, et autres exploits qui menaçaient jusque-là de paralyser l'industrie, ne sont plus qu'une affaire de routine

Lorsque Log4Shell a été annoncé, les entreprises du monde entier se sont empressées de prévenir leurs clients et d'effectuer des mises à jour en urgence sur des centaines ou milliers d'applications. La vulnérabilité Log4Shell (CVE-2021-44228) concerne un environnement logiciel open source appelé Log4j, présent dans des millions d'applications. Le CVSS lui a attribué un score de gravité de 10 sur 10. Dans le cadre du réseau de contenu privé de Kiteworks, néanmoins, le score CVSS de Log4j est de maximum 4, car les API vulnérables de Log4j sont désactivées par Kiteworks et les bibliothèques tierces sont sous haute surveillance lorsqu'elles sont exécutées dans un bac à sable.

Un autre exemple récent est celui des exercices de boîte blanche de Kiteworks, pendant lesquels un chercheur en sécurité, homologué et formé par Kiteworks, a tenté de construire et d'exploiter une chaîne de quatre vulnérabilités, l'une des plus difficiles à concevoir et avec le plus d'impact potentiel. Ce type de vulnérabilité devrait normalement obtenir le score CVSS le plus critique, à savoir 10, et entraîner des mesures correctives immédiates. Cependant, les couches de défense de Kiteworks ont réduit l'exploitabilité et l'impact réels à un score non critique qui n'affecte qu'un petit sous-ensemble de déploiements.