KerioControl

FICHE SYNTHÈSE

Pour les banques et les coopératives de crédit

Segmentation Zero Trust et contrôle audité sur chaque site.

Pare-feu de nouvelle génération et gestion unifiée des menaces déployés sur votre propre infrastructure, en périphérie de chaque site, sans facturation VPN par site.

Tout bloquer par défaut

Toutes les connexions, sur tous les sites, sont bloquées sauf si elles sont explicitement autorisées et associées à une identité vérifiée (AD/LDAP). Un appareil ou des identifiants compromis ne peuvent pas effectuer de mouvements latéraux vers d'autres zones.

Segmentation Zero Trust, par défaut



Comment cela fonctionne : mécanisme de passerelle, puis IA

1 — Déploiement sur site

Appliance virtuelle, matériel appartenant à votre établissement ou appliance dédiée de la série NG : les fonctions de traitement du trafic et d'application des politiques s'exécutent sur une infrastructure contrôlée par votre établissement.

2 — Contrôle d'accès VPN à plusieurs niveaux

Identifiants, puis authentification à deux facteurs, puis vérification d'un appareil de confiance lié au matériel (empreinte composée de 7 attributs, approbation ou révocation par l'administrateur, journal d'audit complet).

3 — Surveillance autonome de la disponibilité

Le watchdog vérifie en continu les services réseau, pare-feu, VPN et IPS, redémarre automatiquement ceux qui échouent et consigne un fichier de vidage mémoire pour analyse, sans nécessiter d'intervention sur site.

4 — Blocage des menaces assisté par IA (Shield Matrix)

L'IA dans le cloud et l'intelligence mondiale issue de honeypots bloquent les adresses IP malveillantes avant qu'elles n'atteignent le réseau ; les informations sur les menaces sont actualisées toutes les 15 minutes, sans charge supplémentaire pour l'appliance.

Conformité : référentiel mondial

Comité de Bâle : principes relatifs au risque opérationnel et à la résilience Basculement haute disponibilité actif/passif (une licence couvre les deux nœuds) et récupération automatique des services réseau essentiels par Watchdog.	Prise en charge
Contrôle d'accès et séparation des tâches (États-Unis : GLBA/FFIEC ; UE : DORA ; Royaume-Uni : FCA/PRA ; Singapour : MAS TRM ; Australie : APRA CPS 234 ; Canada : OSFI B-13) Segmentation Zero Trust « Tout bloquer » avec des règles associées à l'identité, et un journal d'audit complet consignant chaque approbation, refus et révocation d'appareils.	Fonctionnalité
Supervision centralisée de l'ensemble des sites GFI AppManager AI vous permet de gérer plusieurs appliances et de nombreux sites depuis une seule console.	Fonctionnalité

Prêt à commencer ?

Demandez un essai gratuit sur gfi.ai ou contactez le service commercial : sales@gfi.com.

Copyright © GFI USA, LLC. Tous droits réservés.