

Implémentez une protection préventive complète dans vos terminaux pour une entreprise plus sécurisée, durable et résiliente - Simply IGEL It !

11 raisons de choisir IGEL pour sécuriser vos terminaux et espaces de travail virtualisés (VDI, DaaS, SaaS).

Pourquoi IGEL est le meilleur choix de sécurisation de vos terminaux pour Omnisia, Citrix et Azure Virtual Desktop (AVD) :

1. Prévention plutôt que remédiation

Le modèle de sécurité préventive d'IGEL brise le cercle vicieux d'une sécurité reposant uniquement sur la surveillance, la détection et la remédiation de vos terminaux. Ne vous contentez pas de l'IA ou de la détection rapide pour résoudre les problèmes. Éliminez les menaces dès le départ, empêchant ainsi que vos terminaux ne deviennent le point d'entrée pour une attaque de ransomware. Comme l'a récemment mentionné CrowdStrike, les ransomwares commencent et finissent avec le terminal. Utilisez IGEL pour éviter cela.

2. Déplacez Windows vers le cloud

Les offres d'espaces de travail dans le cloud d'Omnissa, Citrix et Microsoft visent à migrer Windows du terminal vers le cloud (privé, public ou hybride). IGEL OS convertit facilement tout terminal x86-64 en un terminal sécurisé et standardisé prêt à accéder au cloud.

3. Supprimez le terminal comme cible des ransomwares

Réduisez l'impact d'une attaque réussie en protégeant les terminaux IGEL avec un chiffrement fort, permettant ainsi aux utilisateurs de se reconnecter dès que les services centraux sont restaurés.

4. Pas de données locales ni de malware sur le terminal

Avec IGEL OS, aucune donnée n'est stockée localement. Que les utilisateurs utilisent leur PC ou un IGEL UD Pocket, toutes les données sont stockées dans le cloud/VDI, soutenant ainsi les initiatives de conformité telles que le RGPD, le CCPA, le CPRA, le CISM, et l'HIPAA.

5. Réduisez votre surface d'attaque

La conception modulaire d'IGEL OS permet d'optimiser les terminaux en excluant les fonctionnalités non nécessaires, minimisant ainsi la surface d'attaque. Pas de bloatware, seulement vos applications spécifiques.

6. Simplifiez et minimisez les mises à jour des terminaux

IGEL OS est modulaire, donc les mises à jour sont spécifiques et sous votre contrôle total, avec des signatures pour une sécurité accrue (même les mises à jour du BIOS sont possibles).

7. Sécurisez le travail à distance, BYOD et les appareils externes

IGEL OS renforce la sécurité pour le travail à distance et le BYOD, garantissant la continuité d'activité même face aux perturbations.

8. Rendez les add-ons de sécurité obsolètes

Les add-ons de sécurité des terminaux sont désormais superflus grâce à la base Linux en lecture seule et le démarrage sécurisé d'IGEL OS.

9. Configuration simple et sécurisée avec UMS

L'Universal Management Suite (UMS) permet aux administrateurs IT de gérer facilement des dizaines de milliers de terminaux avec une configuration simple et personnalisée.

10. Fonctionnalités de sécurité avec plus de 120 partenaires technologiques

Un large écosystème de partenaires intégrant les dernières technologies pour le cloud, VDI, VPN, authentification, sécurité contextuelle, communication unifiée, et plus encore.

Bonus : Réduisez le budget IT et atteignez vos objectifs de durabilité

L'utilisation d'IGEL peut réduire la consommation énergétique de 22 % sur tous vos terminaux, avec des économies supplémentaires grâce à la mise en veille et aux paramètres d'économie d'énergie. Cela contribue aux objectifs environnementaux, sociaux et de gouvernance (ESG) de votre entreprise.

En savoir plus [IGEL Preventative Security Model](#)

Simply IGEL It

IGEL est une marque déposée d'IGEL Technology GmbH.
Tous les noms de matériels et de logiciels sont des marques déposées des fabricants respectifs.
Sous réserve d'erreurs et d'omissions. Sous réserve de modifications sans préavis. © 11/2024

Visitez-nous à [igel.com](https://www.igel.com)

IGEL