

# SAFECONSOLE®

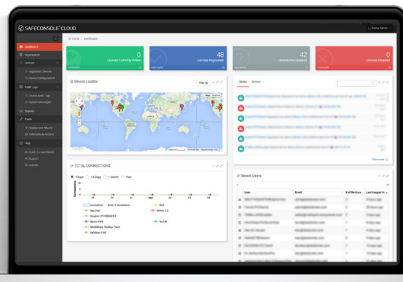
## PLATE-FORME DE GESTION DE CRYPTAGE



GÉRER TOUS VOS  
PÉRIPHÉRIQUES

**SAFECONSOLEReady®**

DEPUIS UN CENTRE DE  
COMMANDE SÉCURISÉ



### NE PERDEZ JAMAIS DE TRACE DE VOS DONNÉES SENSIBLES

Les solutions de cryptage DataLocker permettent de sécuriser les données pour le transport, le stockage et le partage. Maintenant, SafeConsole vous permet de gérer de manière centralisée ces points de connexion, peu importe où ils vont.

SafeConsole est votre centre de commande de stockage sécurisé pour les points de connexion cryptés, y compris les disques durs externes cryptés DataLocker DL3/DL3FE, le lecteur flash crypté DataLocker Sentry® 3 FIPS, la passerelle de cryptage sur le cloud SafeCrypt® et les supports optiques à cryptage automatique EncryptDisc®.\* D'autres produits SafeConsoleReady® incluent des appareils de nos partenaires comme Kingston® Technology et CardWave®.

SafeConsole est idéal pour les employés mobiles qui manipulent des données sensibles ou de la propriété intellectuelle dans plusieurs endroits. SafeConsole vous permet d'administrer des centaines ou des milliers de points de connexion cryptés avec efficacité, visibilité et contrôle.

### FONCTIONNALITÉS DE SAFECONSOLE



**Inventaire.** Surveillez tous vos points de connexion cryptés, y compris leur emplacement partout dans le monde. Intégrez-vous à Active Directory pour suivre facilement les utilisateurs, les périphériques assignés et les ordinateurs connectés.



**Audit.** Voir quels fichiers sont enregistrés ou supprimés de vos points de connexion cryptés à tout moment. Utilisez une piste de vérification complète pour surveiller l'activité par l'utilisateur, y compris les connexions, les échecs de connexion, les réinitialisations et les rapports de perte.



**Contrôle.** Appliquez des règles telles que les règles de mot de passe, les restrictions de type de fichier ou les limites géographiques. Réinitialisez les mots de passe, basculez les points de connexion en mode lecture seule, et même effacez-les à distance en cas de perte ou de vol.



**Rapport.** Obtenez une vue d'ensemble de vos points de connexion cryptés dans le monde entier. Accédez aux rapports par configuration, emplacement géographique, statut, mises à jour, activité récente et plus encore.

### FONCTIONNALITÉS SUPPLÉMENTAIRES

#### GÉOLOCALISATION ET GEOFENCING

Utilisez le suivi d'emplacement basé sur IP pour identifier l'emplacement de vos points de connexion cryptés partout dans le monde. SafeConsole peut également mettre en place une « geofence » pour vos périphériques, ce qui les rend accessibles uniquement dans des limites géographiques spécifiques.

#### DÉPLOIEMENT SIMPLE ET RAPIDE

SafeConsole offre un déploiement facile pour les petites et grandes organisations avec une connexion à Active Directory (AD). Les administrateurs peuvent s'authentifier pour accéder à SafeConsole avec leurs informations d'identification AD. Installez SafeConsole sur votre serveur, puis déployez les lecteurs sur les utilisateurs. Chaque périphérique est enregistré sur un utilisateur spécifique dans SafeConsole et lié à l'utilisateur dans le répertoire de l'entreprise (si disponible).

#### ÉDITEUR

Cette fonctionnalité permet aux administrateurs de déployer ou d'aider au développement des applications et du contenu portables au volume de stockage sécurisé des périphériques gérés.

#### ZONE BUILDER

Zonebuilder est un outil pour créer une « zone de confiance » d'ordinateurs qui rend encore plus simple l'utilisation de vos périphériques gérés SafeConsole.

**🔒 LIMITEZ** l'accès du périphérique aux ordinateurs à l'intérieur de votre zone de confiance.

**🔑 AUTO-DÉVERROUILLEZ** votre périphérique de stockage en éliminant la nécessité d'entrer votre mot de passe. Cette fonctionnalité utilise les certificats client RSA pour l'authentification.

#### SERVICE ANTI-MALWARE

En partenariat avec McAfee, DataLocker offre une protection anti-malware qui s'exécute en arrière-plan de vos périphériques gérés. L'application McAfee scanne le périphérique lors de chaque utilisation, détecte et supprime les logiciels malveillants du périphérique et transmet un rapport à SafeConsole afin que vous sachiez exactement quels périphériques ont été infectés et comment ils ont été désinfectés.

Grâce à McAfee parfaitement intégré dans vos appareils, vous et votre organisation êtes conformes et évitez les incidents pouvant entraîner des coûts élevés de maintenance et de service.

Powered by 

# SAFECONSOLE<sup>®</sup>

## PLATE-FORME DE GESTION DE CRYPTAGE

### GÉREZ DE MANIÈRE CENTRALISÉE L'UTILISATION, LES MOTS DE PASSE, ET PLUS

L'utilisation et l'accès aux périphériques de police en utilisant une vaste gamme de contrôles flexibles de gestion des politiques et des mots de passe.

- Appliquez les règles spécifiques au périphérique pour la longueur et la complexité du mot de passe, la fréquence de changement de mot de passe, le nombre de tentatives, et plus encore.
- Permet aux services d'aide des admins d'aider facilement et à distance les utilisateurs qui ont oublié leurs mots de passe.
- Limitez la capacité d'utiliser des lecteurs sur certains ordinateurs en whitelistant des adresses IP spécifiques ou des plages d'adresses.
- Réinitialisez à distance les périphériques, réinitialiser les politiques de mise à jour des mots de passe, forcez le mode lecture seule, désactivez ou même supprimez les périphériques où que vous soyez dans le monde.
- Activez et administrez le logiciel optionnel de protection anti-virus McAfee sur certains ou sur tous les périphériques que vous gérez.
- See which files are saved to or deleted from your encrypted endpoints at any given moment.
- Restrict which file types are allowed to be stored on the managed devices.



### PÉRIPHÉRIQUES GÉRÉS

**Kingston DataTraveler Vault Privacy 3.0 et DataTraveler 4000 G2**  
Sauvegardez les données sensibles de votre entreprise et protégez les données sensibles par un cryptage AES 256 bits.



**Disques durs externes DataLocker DL3 et DL3 FE**  
Les deux disques durs externes DataLocker définissent une nouvelle norme pour le stockage portable crypté. Aucun logiciel n'est nécessaire pour gérer, crypter ou déployer les disques durs.



**Clé USB DataLocker Sentry 3 FIPS**  
Le Sentry 3 FIPS utilise la technologie certifiée et éprouvée de DataLocker, la certification FIPS 140-2 de niveau 3 et le cryptage AES 256 bits basé sur le matériel.

### OPTIONS DE DÉPLOIEMENT FLEXIBLES

#### SERVICE HÉBERGÉ SUR LE CLOUD

- Mise en route en quelques minutes
- Connectez-vous et gérez partout où vous êtes
- Assistance par email et par téléphone
- Prix par point de connexion/an plus frais de base ponctuels

#### ON-PREM (SUR PLACE)

- Nécessite un serveur dédié basé sur Windows
- Connectez-vous et gérez partout où vous êtes
- Des exigences matérielles et des besoins en bande passantes modestes
- Idéal pour les déploiements de 300 points de connexion ou plus

Consultez [datalocker.com/safeconsole](https://datalocker.com/safeconsole) pour plus de détails, des démos et des tarifs.

### PCI COMPLIANCE

Pour le cloud SafeConsole, nos centres de données ont été certifiés par des normes de sécurité nationales et/ou internationales. De plus, notez que le cloud SafeConsole est une solution à titulaire unique, ce qui signifie que seul le service de votre entreprise est hébergé par ce serveur virtuel spécifique. En outre, aucune donnée réelle des produits de stockage n'est enregistrée sur le cloud. Seule SafeConsole, la console de gestion, est hébergée sur le cloud.

### CONTACT COMMERCIAL

**SITE WEB**  
datalocker.com

**US ET CANADA**  
sales@datalocker.com  
+1 913 310 9088

**EUROPE**  
emea@datalocker.com

**ASIE PACIFIQUE**  
apac@datalocker.com