iStorage®

CLOUDASHUR®

La clé de vos données

CHIFFREZ

pour assurer une protection optimale de vos données stockées dans le cloud, sur votre PC/MAC local ou sur n'importe quel dispositif de stockage

PARTAGEZ

vos données chiffrées en temps réel avec des utilisateurs autorisés, dans le cloud, par e-mail et via des services de transfert de fichiers

GÉREZ

et surveillez vos dispositifs cloudAshur de façon centralisée

Pour garantir la confidentialité des données, le chiffrement est important, et la protection de la clé de chiffrement est vitale. Pour qu'une solution soit véritablement sécurisée, il est impératif que la clé de chiffrement soit conservée à distance des données.

C'est pourquoi nous avons mis au point le Module de sécurité matérielle cloudAshur (brevet en instance). Ce module de sécurité à chiffrement matériel et authentification par code PIN chiffre toutes les données en transit et au repos au moyen d'une clé de chiffrement chiffrée AES 256 bits certifiée FIPS générée aléatoirement. En outre, cette clé est conservée sur un microprocesseur *sécurisé Common Criteria EAL5 + (Hardware Certifié)*.

Aperçu

cloudAshur est la solution idéale pour tous ceux qui veulent stocker, partager, gérer et surveiller en toute sécurité leurs données dans le cloud. cloudAshur élimine les vulnérabilités de sécurité propres aux plateformes cloud, notamment en lien avec le manque de contrôle et les accès non autorisés. Les pirates imaginent d'innombrables méthodes sophistiquées pour cibler les utilisateurs innocents et vulnérables. Bien souvent aussi, l'erreur humaine est à l'origine des incidents de fuites de données.

Le piratage d'un compte cloud peut entraîner le vol et la fuite de données confidentielles, des pertes d'emploi, une publicité négative, de lourdes amendes et potentiellement la chute d'une entreprise.

Suite logicielle iStorage

Application cliente cloudAshur *(Windows et macOS)*

cloudAshur est compatible avec les PC et les Mac et fonctionne avec de nombreux fournisseurs de cloud dont Amazon Drive, Google Drive, OneDrive, Dropbox, iCloud et bien d'autres.

Application cloudAshur KeyWriter *(Windows)*

iStorage KeyWriter (brevet en instance) facilite considérablement le partage de données chiffrées dans le cloud, mais aussi par e-mail et via des services de transfert de fichiers WeTransfer, par exemple) entre des utilisateurs autorisés, en garantissant une sécurité optimale et la tranquillité d'esprit : les données s'échangent en toute sécurité, en temps réel, quel que soit leur emplacement.

Application Remote Management cloudAshur *(Windows)*

La console de gestion à distance Remote Management iStorage cloudAshur offre un contrôle total sur tous les modules de sécurité matérielle cloudAshur déployés dans votre entreprise, et vous donne accès à une large gamme de fonctionnalités pour gérer et superviser tous les utilisateurs.

Toutes les marques déposées et les noms de marque sont la propriété de leurs fabricants respectifs

FONCTIONNALITÉS CLÉS DU MODULE DE CHIFFREMENT CLOUDASHUR

Module de chiffrement cloud avec authentification par code PIN et chiffrement matériel (brevets en instance)

Authentification par code PIN ultra-sécurisé à 7 à 15 chiffres au niveau du module cloudAshur

Puce de chiffrement embarquée

Chiffrement matériel AES-XTS ou AES-ECB 256 bits de niveau militaire 100 % temps réel avec contrôleur de chiffrement certifié FIPS PUB 197.

Mécanisme de défense contre les tentatives de piratage par la force brute

Si le code PIN utilisateur saisi est incorrect 10 fois de suite, il est supprimé et il faut alors saisir le code PIN d'administration pour accéder au disque et réinitialiser le code PIN utilisateur. (L'administrateur peut modifier la limite par défaut de 10 saisies et appliquer une limite entre 1 et 9 saisies, pour le code PIN utilisateur seulement)

Si le code PIN d'administration saisi est incorrect 10 fois de suite, tous les codes PIN ainsi que la clé de chiffrement chiffrée sont définitivement perdus.

Authentification à cinq facteurs

Une chose que vous possédez :

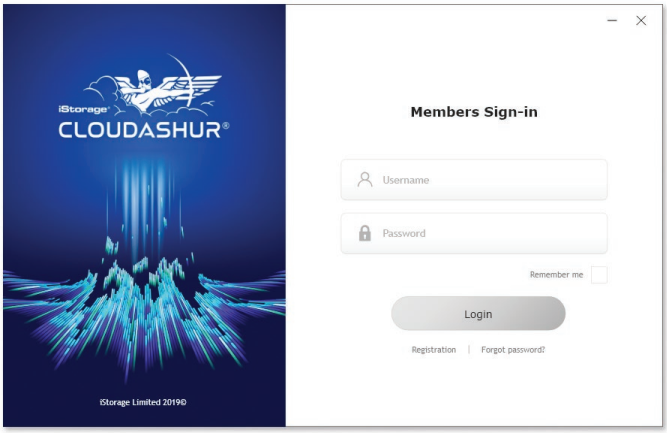
1. *Le module de sécurité matérielle cloudAshur.*

Une chose que vous savez :

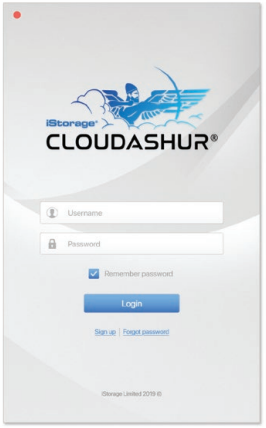
2. *Code PIN à 7 à 15 chiffres configurable par l'administrateur/ l'utilisateur*
3. *Nom d'utilisateur et mot de passe pour l'application cliente iStorage cloudAshur Windows ou MacOS*
4. *Emplacement de stockage des données, fournisseur de cloud*
5. *Nom d'utilisateur et mot de passe du compte cloud*

Compatible avec Windows et macOS

Les applications clientes cloudAshur sont compatibles avec Windows (7/8/10) et macOS (Sierra/High Sierra/Catalina).



(Application cliente Windows)



(Application cliente MacOS)

Deux modes de chiffrement

Le cloudAshur peut être configuré selon deux modes de chiffrement : AES-ECB 256 bits (conforme FIPS) et AES-XTS 256 bits.

Conception anti-sabotage conforme à FIPS 140-2 Niveau 3

Tous les composants critiques situés à l'intérieur du boîtier de cloudAshur sont recouverts d'une couche de résine époxy ultra résistante, qu'il est quasiment impossible de retirer sans endommager définitivement les composants.

En cas de violation, la conception anti-sabotage du module cloudAshur présentera des preuves visibles de l'effraction.

Intègre un microprocesseur sécurisé Critères Communs EAL5 + (Hardware Certifié)

Offre une protection optimale contre le piratage ; détecte et réagit aux tentatives d'effraction grâce à des fonctionnalités telles que :

- *Matériel dédié à la protection contre les attaques SPA/DPA/ SEMA et DEMA*
- *Protection avancée contre les attaques physiques, avec le bouclier Active Shield, le système Enhance Protection Object, le contrôle CStack, le détecteur de pente Slope Detector et les erreurs de parité*
- *Systèmes de protection environnementale contre les fluctuations de tension, de fréquence et de température, et contre la lumière*
- *Gestion sécurisée de la mémoire et protection de l'accès*

Toutes les marques déposées et les noms de marque sont la propriété de leurs fabricants respectifs

iStorage®

FONCTIONNALITÉS CLÉS DU MODULE DE CHIFFREMENT CLOUDASHUR *(suite)*

Revêtement polymère, clavier alphanumérique intégré résistant à l'usure

Le cloudAshur est authentifié (déverrouillé) et toutes les fonctions s'effectuent à l'aide du clavier intégré sans aucune implication de l'hôte. cloudAshur n'est pas vulnérable face aux enregistreurs de frappe ni aux attaques par force brute.

Le clavier du cloudAshur est recouvert d'une couche de polymère résistant à l'usure pour plus de protection.

Ajout aux listes blanches des réseaux

Il possède un VID/PID unique et un numéro de série interne/externe avec code-barres, ce qui permet de l'intégrer facilement dans un logiciel standard de gestion des terminaux (mise sur liste blanche) afin de respecter les exigences des politiques d'entreprise.

Inscription de code PIN utilisateur

L'administrateur peut mettre en place une politique de restriction concernant le code PIN utilisateur. Il peut ainsi définir sa longueur minimale et exiger l'insertion d'un ou plusieurs « caractères spéciaux » s'il le souhaite.

Les « caractères spéciaux » sont de la forme « MAJ (⇧)+ chiffre ».

Verrouillage automatique en cas d'inactivité

Peut être configuré pour se verrouiller après une période d'inactivité prédéfinie. Le cloudAshur se verrouille automatiquement lorsqu'il est débranché de l'ordinateur hôte ou lorsque le port USB n'est plus alimenté.

Immunisé contre les attaques BadUSB

La puce de chiffrement USB et le microprocesseur sécurisés intègrent des mécanismes de verrouillages signés numériques qui immunisent le cloudAshur contre les attaques BadUSB.

Services de personnalisation disponibles

Nous proposons un service de configuration de code PIN en usine et de gravure laser qui permet d'ajouter, sur le manchon ou le côté du module, votre nom, le nom de la société, son logo, une adresse web ou e-mail, ou encore un numéro de téléphone.

Certification IP68

Résistant à la poussière et à l'eau Comprend un manchon de protection rigide en aluminium extrudé anodisé et renforcé

Modes Administrateur et Utilisateur distincts

Permet de créer des codes PIN administrateur et utilisateur indépendants

Fonctionnalité d'autodestruction

Programmez un code PIN d'auto-destruction sur le cloudAshur pour garantir la suppression de la clé de chiffrement chiffrée et de tous les codes PIN.

Code PIN unique de récupération d'utilisateur

L'administrateur peut programmer un code PIN unique de récupération sur le cloudAshur. Cela est extrêmement utile lorsqu'un utilisateur oublie le code PIN lui permettant de s'authentifier sur le cloudAshur.

Cette fonctionnalité permet à l'utilisateur de saisir le code PIN de récupération et de configurer un nouveau code PIN utilisateur.

Voyants LED
ROUGE - en veille / verrouillé
VERT - mode utilisateur / déverrouillé
BLEU - mode administration

Revêtement polymère, clavier alphanumérique résistant à l'usure

Boîtier rigide en aluminium extrudé anodisé et renforcé

Touche MAJ / Bouton Marche-Arrêt

Joint en caoutchouc
Le module devient étanche lorsque le manchon est installé

Intègre un microprocesseur sécurisé Critères Communs EAL5 + (Hardware Certifié)
Offre une protection optimale contre le piratage ; détecte et réagit aux tentatives d'effraction

Revêtement époxy
Tous les composants critiques se trouvant dans le cloudAshur sont recouverts d'une couche de résine époxy ultra résistante

Bouton Clé

Alliage de zinc
(peut être fixé à un porte-clé)

Toutes les marques déposées et les noms de marque sont la propriété de leurs fabricants respectifs

iStorage®

CLOUDASHUR KEYWRITER (BREVET EN INSTANCE)

Facilite considérablement le partage de données entre des utilisateurs autorisés dans le cloud, par e-mail et via des services de transfert de fichiers, en garantissant une sécurité optimale et la tranquillité d'esprit.

FONCTIONNALITÉS DE KEYWRITER

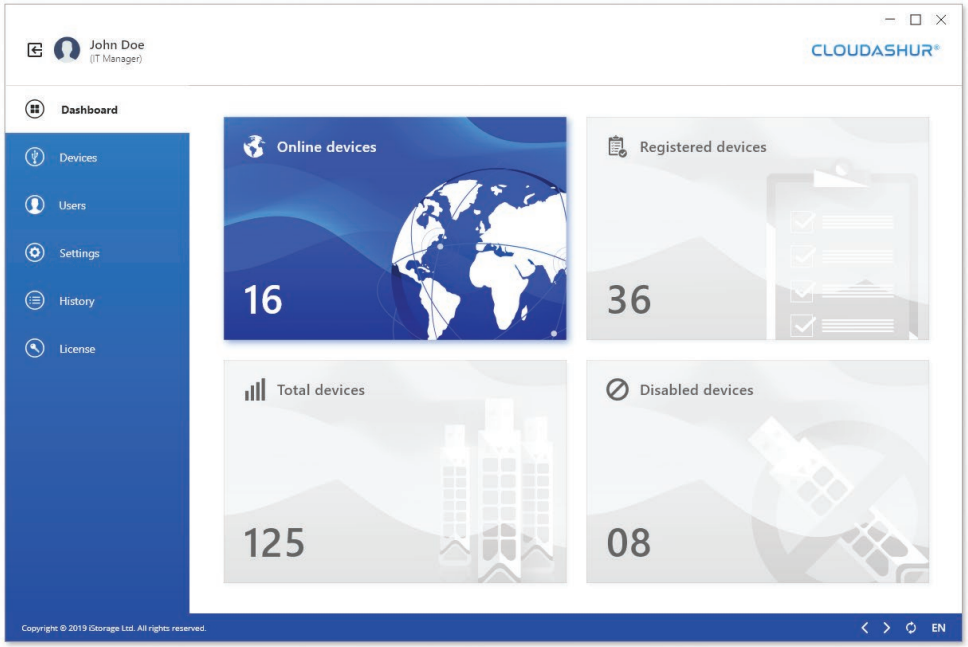
- *iStorage KeyWriter copie tous les paramètres de sécurité critiques, dont la clé de chiffrement générée aléatoirement et l'ensemble des codes PIN, depuis le module cloudAshur maître et vers autant de modules cloudAshur secondaires qu'il le faut, en utilisant n'importe quel hub USB du commerce. Cela permet aux utilisateurs autorisés de partager des données en toute sécurité, en temps réel, quel que soit leur emplacement.*
- *Les paramètres de sécurité critiques ne quittent jamais le module cloudAshur et sont stockés dans le microprocesseur sécurisé Common Criteria EAL5 + (Hardware Certifié).*
- *Le processus de copie de la clé de chiffrement chiffrée et de tous les identifiants entre le module cloudAshur maître et les modules cloudAshur secondaires est protégé par un protocole sécurisé incorporé dans le microcontrôleur sécurisé iStorage cloudAshur. Ce protocole est mis en œuvre à l'aide d'algorithmes cryptographiques, qui sont tous certifiés FIPS. Chaque cloudAshur possède un certificat unique émis par une racine de confiance, qui garantit que seuls des modules iStorage cloudAshur peuvent être utilisés pendant le processus d'échange de clés.*
- *Les modules cloudAshur ne fournissent jamais la clé de session établie au cours du protocole sécurisé, et les données sensibles qui sont copiées ne sont déchiffrées que dans le module cloudAshur de destination qui aura été vérifié. Le logiciel iStorage KeyWriter, qui s'exécute sur un PC, coordonne les opérations requises par le protocole sécurisé. Toutefois, le logiciel n'a aucune visibilité sur la clé de session ni sur les données déchiffrées, ce qui empêche totalement un pirate d'accéder aux paramètres de sécurité critique stockés dans le module cloudAshur ou d'en extraire les données.*

iStorage KeyWriter est compatible avec Windows (*Vista/7/8/10*).

Toutes les marques déposées et les noms de marque sont la propriété de leurs fabricants respectifs

CONSOLE DE GESTION À DISTANCE REMOTE MANAGEMENT CLOUDASHUR

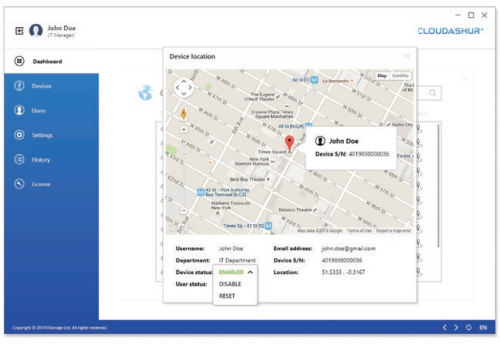
Offre un contrôle total sur tous les modules de sécurité matérielle cloudAshur déployés dans votre entreprise, et vous donne accès à une large gamme de fonctionnalités pour gérer tous les utilisateurs.



FONCTIONNALITÉS DE LA CONSOLE

La console iStorage Remote Management offre à l'administrateur une visibilité et un contrôle complets sur les aspects suivants :

- *Désactivez temporairement ou réinitialisez (fin de processus à distance ou « remote kill ») des modules cloudAshur d'utilisateurs, si vous détectez une activité suspecte ou lorsqu'un collaborateur quitte l'entreprise sans remettre son module de chiffrement cloudAshur.*
- *Limitez les types de fichiers : contrôlez les types de fichiers chargés et partagés dans le cloud (EXE, PNG, PDF, etc.)*
- *Consultez les fichiers de log des utilisateurs : visibilité totale sur les activités de chaque utilisateur dans le cloud, sur les fichiers envoyés, téléchargés, modifiés, etc.*
- *Affichez l'emplacement des utilisateurs : vous pouvez localiser les modules cloudAshur des utilisateurs sur une carte à l'écran.*
- *Bornes géographiques et temporelles : limitez les lieux et les moments auxquels le module de chiffrement cloudAshur peut être utilisé par chaque utilisateur.*



La console iStorage Remote Management est compatible avec Windows (*Vista/7/8/10*).

Toutes les marques déposées et les noms de marque sont la propriété de leurs fabricants respectifs

POURQUOI UTILISER CLOUDASHUR ?

- *Vous conservez la clé de chiffrement de vos données de la façon la plus sûre qui soit ; vous n'avez plus besoin de vous demander si vos données stockées dans le cloud peuvent être consultées, volées ou partagées.*
- *L'authentification à cinq facteurs rend le piratage de vos données quasiment impossible.*
- *Conformité RGPD : les conditions générales des grands fournisseurs de cloud incluent une clause de « limitation de responsabilité » qui fait peser la responsabilité de la sécurité des données sur l'utilisateur ou le client, même lorsque ces données sont stockées sur leurs serveurs. Par exemple, dans ses conditions générales, AWS décline toute responsabilité en cas « d'accès non autorisé aux données, d'altération, de suppression, de destruction, de dommages, de perte ou d'impossibilité de stocker un quelconque contenu ou autres données. » cloudAshur vous apporte la protection ultime : si un pirate parvient à accéder à votre compte cloud, il ne pourra pas déchiffrer vos données.*
- *Si un pirate obtient vos identifiants de connexion au cloud grâce à une technique d'hameçonnage ou autre méthode de piratage sophistiquée, il ne pourra pas déchiffrer vos données.*
- *L'erreur humaine n'est plus un problème.*
- *Protection face au personnel administratif des fournisseurs de cloud qui ont la capacité d'accéder à vos données et contrôlent les clés de chiffrement.*
- *Protection contre les risques liés à la confidentialité des données. Des dizaines de milliers de requêtes de données d'utilisateurs sont envoyées chaque année à Google, Microsoft et d'autres grandes entreprises par des agences du gouvernement. La plupart du temps, ces entreprises fournissent au moins une partie des données.*

Caractéristiques techniques

Matériel	Module de sécurité matérielle (brevet en instance)
Interface	Contrôleur de chiffrement USB 3.0 certifié FIPS PUB 197
Batterie	Batterie rechargeable au lithium polymère 3,7 V
Dimensions (H/L/P)	87,40 mm / 19,40 mm / 13,40 mm
Poids	Sans manchon : environ 28 grammes Avec manchon : environ 37 grammes
Compatibilité	cloudAshur est compatible avec les PC et les Mac et fonctionne avec de nombreux fournisseurs de cloud dont Amazon Drive, Google Drive, OneDrive, Dropbox, iCloud et bien d'autres.
Chiffrement matériel des données	Peut être configuré selon deux modes de chiffrement : AES-ECB 256 bits (conforme FIPS) et AES-XTS 256 bits.
Certifications	FIPS 140-2 Niveau 3, NLNCSA BSPA et Niveau Diffusion Restreinte OTAN (attendue pour les 3e/4e trimestre)
Certifications	
Informations de commande	IS-EM-CA-256
Garantie	3 ans de garantie avec assistance technique gratuite à vie

Conformité au RGPD

Conçu et développé au Royaume-Uni
Assemblé en Chine

Toutes les marques déposées et les noms de marque sont la propriété de leurs fabricants respectifs