

Protiva™ Smart Guardian

||||| Un niveau de sécurité inégalé pour vos données sensibles



ENTREPRISE > PRODUIT

L'un des principaux défis actuels en matière de sécurité des informations réside dans la protection du volume colossal de données privées et confidentielles qui transitent par les entreprises et les administrations publiques. Les clés USB sont particulièrement vulnérables, car la plupart des salariés s'en servent pour conserver des informations sensibles, et elles peuvent facilement être égarées ou subtilisées. Pour une entreprise, l'impact économique des pertes de données peut s'avérer considérable. La réduction de ce risque devient donc une nécessité absolue. C'est dans cette optique que de nombreuses entreprises déploient des solutions personnalisées telles que le chiffrement des données et le contrôle minutieux des ports USB.

En tant que leader de la sécurité numérique, Gemalto offre aux utilisateurs des dispositifs hautement sécurisés pour gérer l'accès individuel aux réseaux, applications et données. Ces systèmes, basés sur des clés de chiffrement, protègent les informations nomades en contrôlant l'accès à la mémoire flash de la clé et en chiffrant les données qui y sont conservées. Les solutions proposées par Gemalto pour la prévention de la perte de données sont faciles à déployer et peuvent être intégrées aux politiques d'entreprise sur la sécurité des ports USB, afin de fournir un niveau de protection des données portables inégalé.

Principales caractéristiques

- Facile et à pratique à utiliser, « plug and play » et compatibilité avec la plupart des systèmes d'exploitation
- Interopérabilité avec les produits de contrôle des points de terminaison disponibles sur le marché
- Prise en charge du standard PKCS#11 de cryptage des cartes à puce et de l'authentification par mot de passe à usage unique.
- Conformité à la Certification FIPS 140-2 niveau 3
- Capacité mémoire de 2 ou 4 Go

Protiva™ Smart Guardian : la simplicité en termes d'utilisation, de déploiement et de gestion

Le dispositif personnel de sécurité Smart Guardian protège vos données portables grâce à la technologie éprouvée des cartes à puce, développée par Gemalto. À la différence des autres produits de stockage numérique USB sécurisés, Smart Guardian fournit un niveau de protection des données inégalé, car toutes les fonctions essentielles et les clés cryptographiques sont gérées en interne, dans l'environnement sécurisé du module de la carte à puce.

Il suffit aux utilisateurs d'insérer le dispositif Smart Guardian dans un port USB, puis de s'authentifier à l'aide d'un mot de passe. Ce

mot de passe est ensuite validé par la carte à puce qui déverrouille le dispositif afin de permettre le transfert, la copie ou l'enregistrement des fichiers confidentiels sur le volume sécurisé, puis leur chiffrement. Une fois la copie terminée, le dispositif peut être verrouillé et retiré en toute sécurité en sélectionnant la commande adéquate depuis le menu contextuel. Protiva™ Smart Guardian offre une solution de sécurité des données complète et personnalisée, facile à déployer et à gérer pour les administrateurs réseau. Ce dispositif est compatible avec la plupart des systèmes d'exploitation et ne nécessite aucun pilote ou logiciel à installer, ce qui rend son adoption rapide et efficace. En cas de saisies erronées successives d'un mot de passe au-delà de la limite définie, le dispositif se bloque automatiquement pour protéger les données contre toute attaque ou tout accès non-autorisé aux clés de chiffrement. Il sera possible, par la suite, de le déverrouiller en mode administrateur, soit au niveau local, soit à distance au moyen d'une procédure d'authentification chiffrée basée sur une infrastructure à clé publique. Smart Guardian est entièrement pris en charge par le « Token Lifecycle Manager », un portail complet pour la gestion des tokens hébergé par Gemalto. Celui-ci permet aux utilisateurs et administrateurs d'enregistrer leurs nouveaux dispositifs, de mettre à jour les logiciels, de modifier les informations d'enregistrement et de verrouiller ou déverrouiller les tokens.

Protiva™ Smart Guardian

IIIIII Un niveau de sécurité inégalé pour vos données sensibles

■ Principaux avantages

> Un niveau de protection des données USB inégalé, grâce à la technologie de cartes à puce

Le module de carte à puce inviolable, intégré au dispositif Smart Guardian, contient un microprocesseur haute performance qui génère les clés de chiffrement utilisées pour chiffrer et déchiffrer les données. Il est donc impossible d'accéder à ces clés de chiffrement, car elles sont protégées par la carte à puce.

En se basant sur la technologie de cartes à puce, Smart Guardian permet d'offrir un niveau de sécurité bien supérieur à celui des clés USB protégées par un code PIN. Bien que d'usage courant, les clés USB sont beaucoup moins sécurisées. Les fonctionnalités de sécurité du module de la carte à puce ainsi que l'architecture sécurisée du logiciel intégré assurent la protection contre les attaques matérielles ou logicielles.

> Renforcement des politiques de sécurité pour les données mobiles

Grâce à une parfaite interopérabilité avec les produits de sécurisation des points de terminaison disponibles sur le marché, Smart Guardian s'avère comme une solution complète contre les pertes de données. Ce dispositif offre un contrôle hautement personnalisé pour toutes les données stockées sur des clés USB et accessibles via le réseau de l'entreprise.

> Coût d'acquisition inférieur par rapport à d'autres solutions

Du fait de son adéquation avec les normes industrielles, sa compatibilité avec la plupart des systèmes d'exploitation et sa technologie de cartes à puce basée sur le standard PKCS#11, Smart Guardian représente un avantage économique considérable



pour les entreprises qui souhaitent déployer des solutions de protection des données portables.

> Adaptation parfaite à l'infrastructure existante

Smart Guardian est doté d'une interface USB standard et fonctionne sous les systèmes d'exploitation Windows et Macintosh, ce qui lui confère une grande souplesse d'utilisation. Associé au portail Token Lifecycle Manager hébergé par Gemalto, il offre une solution complète, facilement intégrable aux infrastructures informatiques existantes.

> Possibilités infinies pour intégrer de nouvelles applications de sécurité

La prise en charge du standard PKCS#11 offre la possibilité d'intégrer de multiples applications au dispositif Smart Guardian, telles que la signature numérique, l'accès sécurisé à distance, l'authentification par mot de passe à usage unique et d'autres services basés sur l'infrastructure à clé publique.

> Sécurité des données renforcée par la technologie de cartes à puce

La technologie de cartes à puce offre plusieurs avantages aux dispositifs de stockage des données sécurisées :

Portabilité et facilité d'utilisation

Les certificats numériques et les clés de cryptage sont toujours conservés sur la carte, et non à l'extérieur. Ce dispositif doté d'une technologie de cartes à puce peut être utilisé depuis n'importe quel système d'exploitation sans compromettre la sécurité.

Accès sécurisé

Seul l'utilisateur autorisé peut avoir accès aux données au moyen d'une authentification à double facteur via le système d'exploitation de la carte à puce.

Chiffrement

Les cartes à puce fournissent de nombreuses fonctionnalités de chiffrement, comme la génération de clés, le stockage de clés sécurisées, la partition des données etc., qui sont utilisées pour protéger les données conservées dans la mémoire flash.

Gestion simple

Les cartes à puce peuvent bloquer l'accès après un nombre prédéfini de saisies erronées du mot de passe. Pour restaurer l'accès, une procédure rigoureuse d'authentification chiffrée basée sur l'infrastructure à clé publique doit être utilisée. Ce système interdit l'accès non-autorisé aux clés de cryptage et protège l'utilisateur autorisé.



www.gemalto.com

gemalto
security to be free