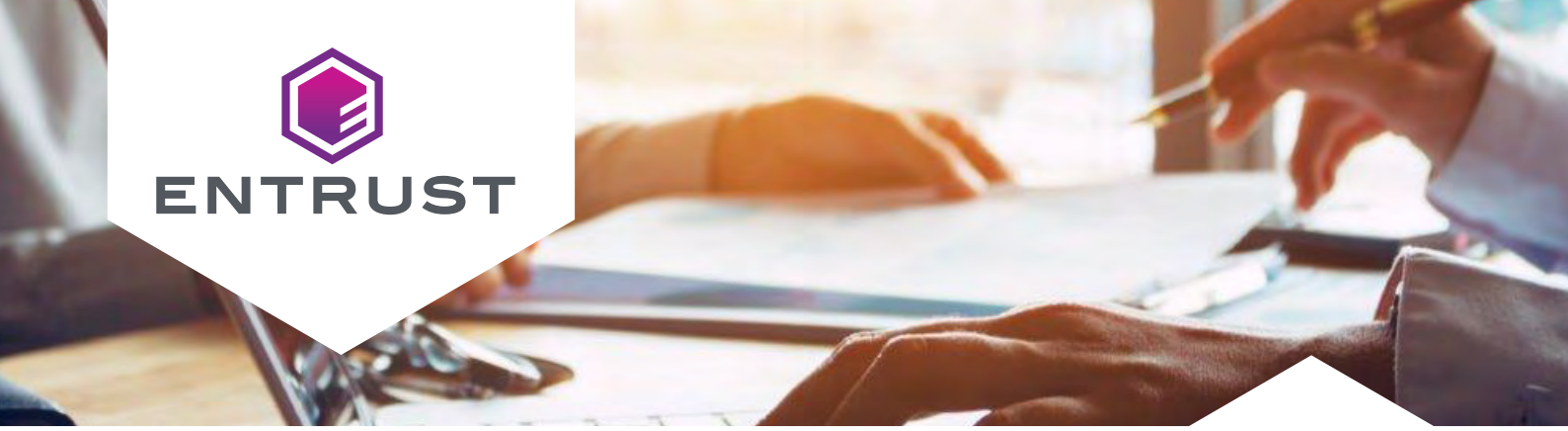

Entrust et les principaux fournisseurs de bases de données renforcent la sécurité des données et la conformité

NFINITY
STRATEGIC TECHNOLOGY PARTNER PROGRAM

Des bases de données hautement protégées grâce aux modules matériels de sécurité (HSM) nShield

CARACTÉRISTIQUES

- Protéger les données inactives pour les déploiements sur site et basés sur le cloud
- Répondre aux politiques strictes de sécurité des données et aux mandats de conformité
- Renforcer la sécurité en séparant les clés des bases de données
- Gérer de manière centralisée les clés de chiffrement, les politiques et les accès
- Sécuriser les clés de chiffrement dans un module matériel de sécurité certifié FIPS 140-2 niveau 3 et Critères communs EAL4+ inviolable

Le défi :

Les entreprises utilisent des bases de données avancées pour héberger des données sensibles comme les informations personnelles des consommateurs, la propriété intellectuelle et les registres financiers. Sans une protection adaptée, les organisations peuvent être confrontées à une atteinte à leur réputation, à un non-respect de la conformité et à des conséquences financières importantes en cas de violation. Les organisations protègent généralement ces données inactives importantes en utilisant les capacités de chiffrement transparent des données (TDE) ou de chiffrement au niveau cellule (CLE) qui sont inhérentes aux principales offres de bases de données.

Selon le type de base de données, le chiffrement peut être mis en œuvre au niveau de la base de données, du tablespace, de la colonne ou de la cellule, et de nombreuses organisations chiffrent également les journaux et rapports associés qui peuvent contenir des informations sensibles. Cela signifie que les clés utilisées pour chiffrer ces fichiers et bases de données sont essentielles à la protection, et ne doivent jamais tomber entre de mauvaises mains. Le vol ou la perte des clés pourrait entraîner la divulgation des registres de la base de données, ce qui entraînerait un préjudice financier pour cause de non-respect de la conformité.

Pour assurer une protection robuste des clés de chiffrement, celles-ci doivent être isolées des biens qu'elles protègent et être gardées d'une manière conforme aux réglementations sur la protection des données et aux meilleures pratiques de l'industrie. Dans le même temps, les clés doivent toujours être facilement disponibles pour assurer une performance optimale de la base de données et des applications qui reposent sur son contenu.

Des bases de données hautement protégées grâce aux HSM nShield

La solution : un chiffrement de la base de données intégré grâce aux HSM nShield

Les modules matériels de sécurité (HSM) nShield de Entrust s'intègrent avec les principaux fournisseurs de bases de données afin de fournir la racine de confiance pour les clés de chiffrement des bases de données.

Grâce aux HSM nShield de Entrust, les clés principales utilisées pour protéger les clés de chiffrement des bases de données bénéficient d'un niveau de sécurité supplémentaire. Les HSM nShield offrent une sécurité certifiée FIPS 140-2 niveau 3 et Critères Communs EAL4+ pour vos clés essentielles sans avoir besoin de modifier des applications, structures de bases de données ou processus existants.

La protection des clés est assurée par une politique qui réduit la probabilité d'une attaque d'initié et minimise le risque de violation des données. Cette combinaison offre une sécurité vérifiable et favorise la conformité aux mandats réglementaires et législatifs, notamment la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS).

Pourquoi choisir nShield

Les HSM nShield facilitent la protection et la gestion des clés de chiffrement des bases de données grâce à des options de déploiement flexibles, notamment le regroupement et le basculement. Ces capacités assurent la continuité des systèmes critiques, conformément à vos besoins en matière de récupération après incident et de conservation des données.

Disponibles sous forme de carte dédiée pour les applications à serveur unique ou sous forme d'appareil sur réseau partagé pour les environnements virtualisés, les HSM nShield séparent la gestion des politiques de sécurité des fonctions administratives, vous aidant ainsi à répondre aux exigences évolutives de votre entreprise.

Avantages des HSM nShield :

- Protection matérielle des clés – Permet de stocker les clés de chiffrement des bases de données au sein d'un environnement sécurisé inviolable isolé de la gestion de la base de données afin d'éviter toute copie ou sabotage
- Application des utilisateurs et des rôles – Étendre les droits d'accès établis dans les bases de données pour accéder aux données chiffrées
- Contrôle rigoureux des clés – Authentification des administrateurs par carte à puce afin de contrôler l'accès aux clés de chiffrement des bases de données
- Séparation des rôles – Répartition de la responsabilité des tâches et procédures importantes entre plusieurs administrateurs
- Soutien à la conformité – Conformité aux mandats exigeant une forte protection des informations sur les clients

Partenariat nFinity

Microsoft SQL Server · IBM DB2 · ORACLE DATABASE

En savoir plus

Pour en savoir plus sur les HSM nShield de Entrust, rendez-vous sur **entrust.com/fr/HSM**
Pour en savoir plus sur les solutions de protection numérique de Entrust pour les identités, l'accès, les communications et les données, rendez-vous sur **entrust.com/fr**

Découvrez-en plus sur
entrust.com/fr/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com