LIVRE BLANC

Guide complet de la sécurisation des données grâce au chiffrement des bases de données

Aujourd'hui, les entreprises demandent à leurs équipes de sécurité de prendre en charge l'expansion rapide de différents cas d'utilisation du chiffrement des bases de données. Ce livre blanc aborde en détails les raisons pour lesquelles la demande de chiffrement des bases de données n'a jamais été aussi forte et les défis qu'elle représente. Ce livre blanc vous donne un aperçu des principales méthodes à adopter pour faire face à cette demande accrue. Il mentionne également les différents types de méthodes de chiffrement disponibles afin d'aider les responsables de la sécurité à s'assurer qu'ils utilisent les outils adéquats à bon escient. Enfin, ce livre blanc vous propose de découvrir la gamme de solutions SafeNet de Gemalto pour la protection des données. Il vous explique comment ces solutions permettent aux équipes de sécurité de remplir leurs objectifs de sécurisation des bases de données de manière efficace et globale.

Pour quelles raisons la demande de chiffrement des bases de données est-elle devenue aussi forte et aussi compliquée ?

Aujourd'hui, la majorité des entreprises modernes stockent la quasi-totalité de leurs actifs numériques critiques dans des bases de données d'entreprise. Il n'est pas surprenant de constater que ces référentiels sont les cibles privilégiées des collaborateurs mal intentionnés et des cyber-criminels. Il va sans dire qu'une base de données corrompue peut se révéler catastrophique en terme de stratégie et de sanctions financières pour les entreprises qui en sont victimes.

Dans ce contexte, les stratégies de sécurité d'entreprise et les exigences réglementaires insistent de plus en plus sur l'importance du chiffrement pour assurer la protection des données se trouvant dans les bases de données.

Toutefois, cette demande de plus en plus pressante à sécuriser les données dans les bases de données ne se fait pas sans poser de nombreux défis. Tandis que l'on assiste à une utilisation de plus en plus grande du « Big data », il en va de même pour le nombre de référentiels différents qui accèdent et exploitent les bases de données. En conséquence, un nombre considérablement plus grand de systèmes doivent être sécurisés et leur défense assurée contre les vecteurs de menace potentiels. Les entreprises se reposent de plus en plus sur une gamme extrêmement variée de modèles informatiques internes, externes et hybrides. Ceci signifie que la sécurité d'un nombre encore plus grand de bases de données doit être assurée au sein d'environnements variés et d'écosystèmes de plus en plus complexes. Par ailleurs, des niveaux de défense supplémentaires doivent être mis en place pour atténuer les risques inhérents aux environnements Cloud, notamment les niveaux supplémentaires de risques administratifs et d'exposition potentielle aux dangers lorsqu'un fournisseur de services Cloud est assigné en justice. Alors qu'elles essayent de composer avec cette demande de plus en plus urgente de chiffrement des bases de données, la majorité des équipes de sécurité sont freinées dans leur mission par les outils et méthodes déjà en place. De nombreuses entreprises ont adopté une approche tactique de la mise en place du chiffrement motivée par les efforts d'équipes projet spécifiques, par les exigences réglementaires et par les silos technologiques. Cette approche a laissé place à la mise en place d'un chiffrement dfficilement déployable et administrable de manière centralisée. Ceci est particulièrement vrai lorsqu'il s'agit de la gestion de clés. En effet, la nature disparate et fragmentée de ces déploiements a fait surgir un grand nombre de nouveaux défis, notamment la prolifération des banques de clés, l'augmentation des coûts et l'apparition de nouveaux risques.

Comment chiffrer les données dans les bases de données?

Le besoin : une approche globale de la protection des bases de données

Pour faire face à tous les défis mentionnés ci-dessus, il est essentiel que les équipes de sécurité des entreprises établissent des stratégies de protection plus ciblées dans toute l'entreprise. Par conséquent, les équipes de sécurité doivent utiliser des plates-formes qui leur font bénéficier d'une administration centralisée des clés et des stratégies performantes dans toute l'entreprise. Elles doivent aussi pouvoir bénéficier de différentes fonctionnalités et de solutions souples pour pouvoir appliquer le chiffrement de manière optimale quel que soit le cas d'utilisation.

Exigences globales

Quelle que soit la solution utilisée, celle-ci doit offrir aux équipes de sécurité les fonctionnalités essentielles suivantes :

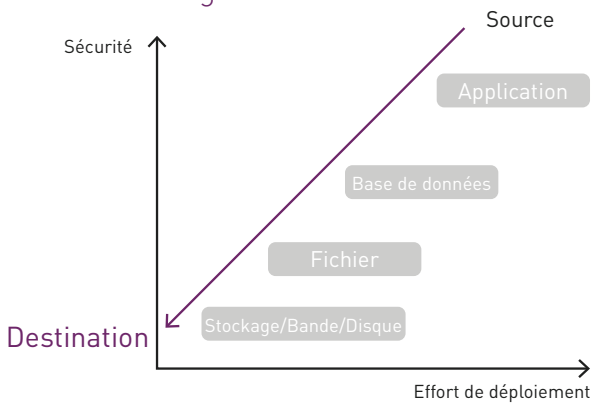
- Sécurisation des données et contrôle de l'accès à ces données.
- Application de contrôles d'accès rigoureux pour assurer la protection des clés et pour les gérer de manière efficace tout au long de leur cycle de vie.
- Stockage et gestion des clés de manière à ce qu'elles soient physiquement et logiquement isolées des référentiels de données.

Quelle est la bonne méthode à adopter pour chaque cas d'utilisation?

Les équipes de sécurité peuvent choisir parmi de nombreuses méthodes et solutions différentes pour chiffrer les données des bases de données. Il faut en effet sélectionner les solutions capables de faire face aux attaques les plus dangereuses tout en prenant également en compte les coûts, les efforts d'intégration et d'administration, les niveaux de services d'utilisation et la simplicité d'utilisation. Retrouvez ci-dessous un aperçu des méthodes disponibles ainsi que leurs points forts et leurs points faibles :

- **Chiffrement et tokénisation au niveau des applications.** Grâce au chiffrement et à la tokénisation au niveau des applications, les entreprises arrivent souvent à bénéficier des plus hauts niveaux de sécurité. Cette méthode permet aux entreprises de sécuriser leurs données sensibles tout au long de leur cycle de vie (du jour de leur création ou de leur capture jusqu'à leur suppression). Toutefois, cette méthode nécessite en général un effort très important de mise en place.
- **Chiffrement des bases de données.** Grâce au chiffrement des bases de données, les entreprises peuvent assurer la sécurité de colonnes spécifiques dans la base de données. Par exemple, elles pourraient vouloir chiffrer une colonne contenant les numéros de sécurité sociale des employés tout en laissant les autres données en clair. Cette méthode est plus facile à mettre en place que le chiffrement des applications. En revanche, elle ne permettra probablement pas de faire face au même nombre de menaces potentielles.
- **Chiffrement des systèmes de fichiers.** Cette méthode permet aux entreprises de chiffrer tout le fichier de la base de données. Cette méthode n'offre pas le même niveau de protection que la méthode de chiffrement des applications et des bases de données. Par contre, elle peut s'avérer être le meilleur moyen pour sécuriser les fichiers de bases de données avant ou pendant les opérations d'exportation, de sauvegarde et d'archivage dans les emplacements de stockage. Par rapport aux méthodes précédentes, cette alternative se révèle bien souvent plus facile à utiliser et à gérer.

Où chiffrer et gérer les clés?

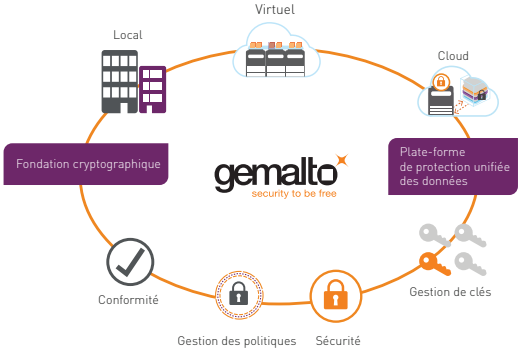


En général, le chiffrement à un niveau plus élevé de la pile informatique permet de bénéficier d'une plus grande sécurité mais impose de plus grands efforts de déploiement.

Solutions SafeNet de protection des bases de données

La gamme de solutions de protection des données SafeNet de Gemalto permet à votre entreprise de mettre en place une méthode stratégique complète de protection des données de la base de données dans toute votre entreprise. La société offre une gamme complète de solutions de chiffrement et de tokénisation ainsi que des solutions de gestion des clés qui permettront à votre équipe de sécurité de gérer efficacement tous les déploiements et clés de chiffrement de votre entreprise. Les solutions de protection de données SafeNet sont les seules solutions du marché à offrir les avantages suivants :

Protection unifiée des données



Gemalto offre un gamme complète de solutions de protection unifiée des données dans toute l'entreprise.

- **Gestion centralisée et fiable des clés.** Toutes les solutions de protection des données SafeNet sont déployées avec SafeNet KeySecure qui offre la gestion centralisée et hautement sécurisée des clés de chiffrement dans toute l'entreprise. En offrant la gestion centralisée des clés et des stratégies et des fonctions de rotation de clés automatisée et de régénération de clés, la solution renforce votre sécurité tout en réduisant vos efforts administratifs.
- **Installation et fonctionnement performants.** Les solutions de protection des données SafeNet offrent l'administration centralisée, la gestion des stratégies et des fonctions d'audit et d'édition de rapports permettant une meilleure application des stratégies et facilitant les tâches d'administration. Grâce à ces solutions, vous bénéficiez d'une architecture plus efficace qui réduit au minimum l'impact du chiffrement sur les performances.
- **Compatible avec de nombreux environnements.** Ces solutions sont compatibles avec un grand nombre d'environnements et modèles informatiques, incluant notamment divers services Cloud public, systèmes virtuels, centres de données traditionnels, infrastructures hybrides et les déploiements de type Big Data.
- **Compatible avec le chiffrement multi-niveaux.** Les solutions de protection des données SafeNet permettent aux équipes de sécurité d'utiliser différentes méthodes, notamment le chiffrement de colonnes, de fichiers et de dossiers et de toutes les machines ou instances virtuelles. La suite de produits propose des solutions de chiffrement et de tokénisation des bases de données et des applications.
- **Compatible avec toutes les bases de données.** Les solutions SafeNet permettent à votre entreprise de chiffrer les données dans les bases de données non SQL (Cassandra, MongoDB et HBase) et dans les bases de données SQL (Microsoft SQL Server, Oracle, IBM DB2, MySQL et PostgreSQL).

Solutions de protection des colonnes sélectionnées dans les bases de données

SafeNet ProtectDB : chiffrement des colonnes
SafeNet ProtectDB offre le chiffrement des colonnes de données structurées et des bases de données SQL. SafeNet ProtectDB permet aux entreprises de remplir leurs objectifs de sécurité, notamment la sécurisation des données financières, la conformité à la norme PCI DSS et la protection des données d'identification personnelle.

La solution inclut des fonctionnalités transparentes et performantes de chiffrement. SafeNet ProtectDB permet aux équipes de sécurité de mettre en place des contrôles d'accès rigoureux par rôle, par utilisateur, par heure du jour et à l'aide d'autres variables. La solution offre de solides défenses qui permettront, par exemple, à votre équipe de sécurité d'empêcher un administrateur de bases de données d'utiliser l'identité d'un autre utilisateur pour accéder aux données sensibles. Pour renforcer la sécurité, les fonctions de rotation de clés automatisée et de régénération de clés ainsi qu'une interface centrale pour la journalisation et l'édition de rapports sont intégrées à la solution.

SafeNet ProtectApp : chiffrement des applications
SafeNet ProtectApp chiffre les données dans l'application avant qu'elles ne soient enregistrées sur la base de données. La solution offre également une interface de gestion des clés.

La majorité des entreprises ont recours à SafeNet ProtectApp pour sécuriser leurs informations sensibles (propriété intellectuelle ou données d'identification personnelles) et pour satisfaire aux exigences de conformité et réglementaires.

La solution est compatible avec les bases de données SQL et non SQL et assure la protection des données structurées et non structurées. Le chiffrement s'effectue sur la plate-forme SafeNet KeySecure afin d'assurer des performances optimales et de permettre la gestion centralisée des clés et des stratégies.

SafeNet ProtectApp permet aux entreprises de sécuriser de manière transparente leurs données tout au long de leur cycle de vie, quel que soit l'endroit où elles sont envoyées, stockées ou copiées. La solution offre les fonctions suivantes :

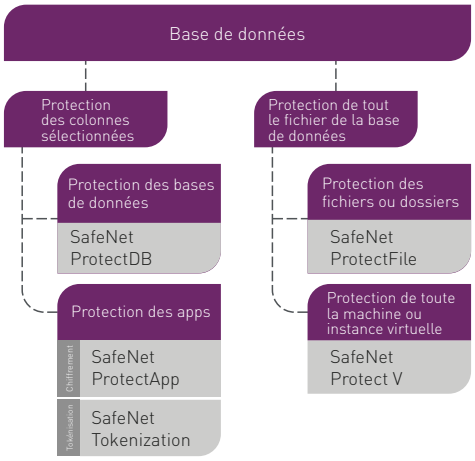
- APIs permettant de simplifier l'intégration sur les infrastructures de serveur d'applications de divers éditeurs.
- Contrôles d'accès rigoureux permettant aux équipes de sécurité de s'assurer que seuls les utilisateurs et applications autorisés ont accès aux données déchiffrées.
- Fonctions complètes d'audit et de journalisation.
- Fonctions de rotation de clés automatisée et de régénération de clés intégrées.

SafeNet Tokenization : tokénisation des applications
Lorsque les entreprises utilisent SafeNet Tokenization, elles peuvent remplacer les éléments sensibles composants les données par un token qui, en cas d'accès, n'offrira aucune valeur ou signification. La solution procède à la tokénisation des données avant qu'elles ne soient stockées dans une base de données.

SafeNet Tokenization offre une grande souplesse d'utilisation de formats normalisés ou personnalisés. Les fonctionnalités de préservation du format lors de la tokénisation vous permettent d'assurer que les données remplacées par des tokens conservent les mêmes propriétés que la valeur d'origine. De cette manière, l'impact potentiel sur les processus et applications pouvant accéder aux données est réduit au minimum. SafeNet Tokenization inclut des contrôles d'accès rigoureux et des fonctions complètes de journalisation et d'audit. La solution offre tout un éventail de fonctionnalités pour simplifier le déploiement, notamment la prise en charge des services Web, la tokénisation en série et la compatibilité avec les lots d'API.

SafeNet Tokenization peut être utilisée pour la tokénisation de tous les types de données sensibles, notamment les numéros de compte, les numéros de carte de crédit, les numéros de sécurité sociale et bien d'autres encore. La majorité des entreprises utilisent SafeNet Tokenization pour sécuriser les numéros de compte de carte de paiement principale afin de se mettre en conformité avec la norme PCI DSS (Payment Card Industry Data Security Standard). En outre, la solution permet aux entreprises de protéger les données d'identification personnelle et les données sensibles dans les environnements Big Data. Enfin, les entreprises peuvent utiliser la solution pour sécuriser les données sur les environnements hors production et notamment ceux utilisés pour le développement, le test et la recherche d'applications et bien d'autres encore.

Options de chiffrement des bases de données



La gamme de solutions de protection des données SafeNet permet aux entreprises de bénéficier de toute une série de méthodes de sécurisation des données dans les bases de données.

Solutions de protection de tout le fichier de la base de données

SafeNet ProtectFile : chiffrement des systèmes de fichiers
SafeNet ProtectFile applique le chiffrement sur tout le fichier de la base de données de façon transparente. La solution est compatible avec les bases de données SQL et non SQL et elle chiffre les fichiers non structurés. SafeNet ProtectFile permet aux équipes de sécurité d'utiliser les protocoles de partage de fichiers tels que CIFS (Common Internet File System) et NFS (Network File System) pour sécuriser les fichiers de base de données se trouvant sur les environnements de stockage direct DAS, les réseaux de stockage SAN et les serveurs de stockage en réseau NAS.

La solution offre de solides défenses contre les menaces internes, en empêchant, par exemple, les administrateurs malveillants d'usurper l'identité d'un autre utilisateur pour accéder aux données chiffrées. Pour renforcer la sécurité, les fonctions de rotation de clés automatisée et de régénération de clés ainsi qu'une interface centrale pour la journalisation et l'édition de rapports sont intégrées à la solution.
SafeNet ProtectFile est une solution optimale de sécurisation des

SafeNet Database Protection Solutions at a Glance				
Solution	Niveau/type de mise en place	Bases de données	Types de données	Environnements
SafeNet ProtectApp	Chiffrement des applications	Non SQL et SQL	Structurées et non structurées	> Environnements Cloud public > Environnements virtuels > Centres de données traditionnels > Environnements hybrides > Déploiements de type Big Data
SafeNet Tokenization	Tokénisation des applications	Non SQL et SQL	Structurées	
SafeNet ProtectDB	Chiffrement des colonnes	SQL	Structurées	
SafeNet ProtectFile	Chiffrement des fichiers et dossiers	Non SQL et SQL	Non structurées	
SafeNet Transparent Data Encryption	Chiffrement des fichiers et dossiers	SQL	Structurées	
SafeNet ProtectV	Chiffrement des machines virtuelles	Non SQL et SQL	Non structurées	Les environnements virtuels et Cloud public notamment Amazon Web Services, Microsoft Azure, IBM SoftLayer Cloud et VMware

fichiers de base de données, notamment les fichiers utilisés pour les exportations, les archives et les sauvegardes. La solution assure également une sécurité efficace des déploiement de type Big Data, notamment ceux fonctionnant sous Apache Hadoop et IBM InfoSphere Big Insights.

SafeNet ProtectV : chiffrement intégral des disques de machines virtuelles

SafeNet ProtectV permet aux entreprises de chiffrer l'ensemble de la machine virtuelle, notamment les volumes de stockage associés, les instantanés (snapshots) et sauvegardes d'instance et les partitions. La solution chiffre les fichiers non structurés dans les bases de données non SQL et SQL.

La solution permet aux entreprises de sécuriser efficacement les environnements virtuels et Cloud. Les équipes de sécurité sont en mesure de garder en permanence la propriété et le contrôle des données et des clés de chiffrement. Elles peuvent mettre en place des contrôles afin d'autoriser le lancement des instances ou machines virtuelles. Elles peuvent également auditer et signaler tous les accès aux clés et révoquer les droits d'accès aux clés en cas de violation de sécurité. SafeNet ProtectV fonctionne avec SafeNet KeySecure pour offrir la gestion centralisée des clés et des stratégies.

Gestion centralisée et fiable des clés d'entreprise

SafeNet KeySecure

SafeNet KeySecure est une plate-forme certifiée par la norme FIPS 140-2 qui vous permet de créer un service cryptographique centralisé pour simplifier les déploiements du chiffrement dans toute votre entreprise. SafeNet KeySecure s'intègre facilement avec la suite de solutions de chiffrement SafeNet, notamment SafeNet ProtectApp, SafeNet ProtectDB, SafeNet ProtectFile, SafeNet ProtectV et SafeNet Tokenization.
SafeNet KeySecure offre également une vaste gamme d'API et de bibliothèques de développement standard et prend en charge la norme KMIP (Key Management Interoperability Protocol). Votre entreprise peut donc procéder à un déploiement efficace et rapide quel que soit le moment, l'endroit ou la manière dont vous souhaitez intégrer le chiffrement.

Gestion transparente des clés de chiffrement des données avec SafeNet KeySecure

Aujourd'hui, la majorité des versions de bases de données Oracle et Microsoft SQL Server proposent la fonctionnalité de chiffrement transparent des données (TDE) qui permet aux entreprises de procéder au chiffrement des données dans les bases de données. Toutefois, lorsque la fonctionnalité de chiffrement transparent des données est utilisée, les clés cryptographiques générées sont stockées dans la base de données avec les données chiffrées. L'entreprise est donc vulnérable aux violations de sécurité et aux échecs de ses audits de conformité. SafeNet KeySecure permet aux entreprises de bénéficier des fonctionnalités natives du chiffrement transparent des données tout en gérant les clés séparément et de manière beaucoup plus sécurisée. De plus, cette méthode est transparente pour les applications et les utilisateurs accédant aux données sécurisées.

Conclusion

Aujourd'hui, les entreprises doivent répondre à une demande de plus en plus pressante à sécuriser les données dans les bases de données. La gamme Gemalto de solutions de protection des données SafeNet permet à votre entreprise de bénéficier de toutes les fonctionnalités dont elle a besoin pour répondre à cette demande et de le faire avec un niveau d'efficacité encore inégalé. Ces solutions vous permettent d'exploiter toutes les fonctionnalités de gestion centralisée et unifiée des clés et stratégies toute en mettant en place des méthodes de protection des bases de données parfaitement adaptées aux risques spécifiques auxquels doit faire face votre entreprise, à ses technologies, aux exigences réglementaires qu'elle doit respecter et à ses objectifs commerciaux.

À propos de Gemalto

Grâce à l'acquisition de SafeNet, Gemalto offre désormais l'une des gammes de solutions de sécurité pour entreprise les plus complètes du marché. Ses clients bénéficient de solutions de pointe en matière de protection des identités, paiements, transactions et données numériques, de la périphérie au cœur des réseaux. La gamme récemment étendue de solutions de protection des identités et des données SafeNet de Gemalto permet aux entreprises présentes sur de nombreux marchés, notamment les plus grandes institutions financières et les organismes gouvernementaux, de se concentrer sur la sécurité de leurs données à l'aide de méthodes de chiffrement novatrices, de techniques de gestion cryptographique de pointe et de solutions d'authentification forte et de gestion d'identité qui protègent ce qui est important, là où c'est important. Grâce à toutes ces solutions, Gemalto aide les entreprises à se conformer aux réglementations les plus strictes en matière de confidentialité des données. Elle s'assure également que les actifs sensibles des entreprises, leurs bases de données clients et leurs transactions numériques sont à l'abri de toute divulgation et de toute manipulation afin de préserver la confiance des clients dans un monde de plus en plus numérique.

Nous contacter : retrouvez toutes les coordonnées de nos filiales sur www.safenet-inc.com

Nous suivre : data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free