THALES

cpl.thalesgroup.com

Le chiffrement intégral

Guide pratique pour apprendre à protéger les données sensibles de votre organisation

Table des matières

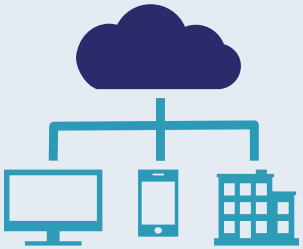
Aperçu

En tant qu'expert en matière de sécurité des données pour votre entreprise, vous devez protéger les données sensibles de votre organisation en développant et appliquant une stratégie de chiffrement à l'échelle de l'entreprise. Mais il est très difficile d'identifier où résident les données sensibles de votre entreprise. On retrouve des données critiques partout. Les limites ont disparu depuis longtemps. Les données circulent des systèmes opérationnels aux systèmes d'analyse, des sites vers le cloud et des bases de données vers les data lakes (ou lacs de données). Le monde des données évolue à une rapidité encore jamais vue ; de nouvelles technologies, comme le big data et les micro services, sont adoptées simultanément et de différentes façons.

Les équipes de sécurité IT sont à la recherche d'une approche holistique pour résoudre les défis actuels liés à la sécurité des données, avec une plateforme de sécurité des données qui leur permette d'identifier et de protéger les données sensibles où qu'elles se trouvent grâce à une gamme complète de méthodes de protection des données et une gestion centralisée des stratégies et des clés. Cet eBook offre un aperçu des méthodes et meilleures pratiques pouvant être utilisées pour définir et appliquer des politiques de sécurité des données afin de découvrir, classifier et protéger vos données les plus sensibles.

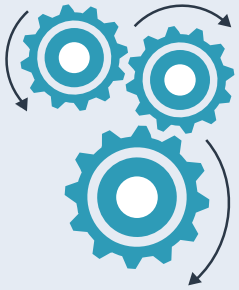
Les défis relatifs à la sécurité des données

Il existe quatre défis majeurs en matière de sécurité des données :



Croissance exponentielle du volume de données

Nouvelles exigences de conformité



Complexité opérationnelle

Menaces en augmentation rapide

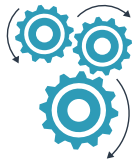
Les plus grands défis relatifs à la sécurité des données

Croissance exponentielle des données

Indépendamment de leur taille, secteur ou localisation dans le monde, les entreprises produisent plus de données que jamais auparavant. Parallèlement, la demande d'accès à cette information est croissante. Tout le monde veut accéder aux données, des équipes de business intelligence et de marketing, aux partenaires et fournisseurs tiers. Elles permettent de réduire les coûts, d'améliorer l'efficacité, de développer de nouveaux produits, d'optimiser l'offre et de prendre des décisions commerciales plus intelligentes et axées sur des données. Pour satisfaire ces demandes, la production, le stockage, le traitement, le partage et la distribution des données surviendront à divers endroits.

De nouvelles exigences de conformité

Afin de répondre aux menaces mondiales changeantes pesant sur les données personnelles (personally identifiable information ou PII), toujours plus de mandats de conformité sont développés afin de renforcer la protection des données sensibles contrôlées et traitées par les entreprises. On dénombre parmi ces derniers le Règlement Général sur la Protection des Données (RGPD), la loi californienne sur le respect de la vie privée des consommateurs (CCPA) et la loi brésilienne Lei Geral de Proteção de Dados (LGPD), entres autres. Les organisations ont cependant besoin de conseils pour répondre à certaines exigences et être en conformité avec ces règlements et mandats de l'industrie, tel que le PCI DSS.



Complexité opérationnelle

La circulation des données entre le cloud, les conteneurs, les technologies big data et les divers outils des nombreux fournisseurs complexifie tout. Les périmètres de sécurité des entreprises sont de plus en plus flous, et par conséquent, les organisations ont de plus en plus de mal à pouvoir payer des politiques d'accès unifiées et cohérentes, ainsi qu'à les appliquer, les gérer et les distribuer aux différentes ressources informatiques. Chaque organisation dispose d'un mélange de plateformes nouvelles et anciennes. Cependant, quels que soient les compartiments en question, les données restent des données. La perte de données sensibles reste une perte de données sensibles quel que soit l'endroit où elle survient.

Des menaces en augmentation rapide

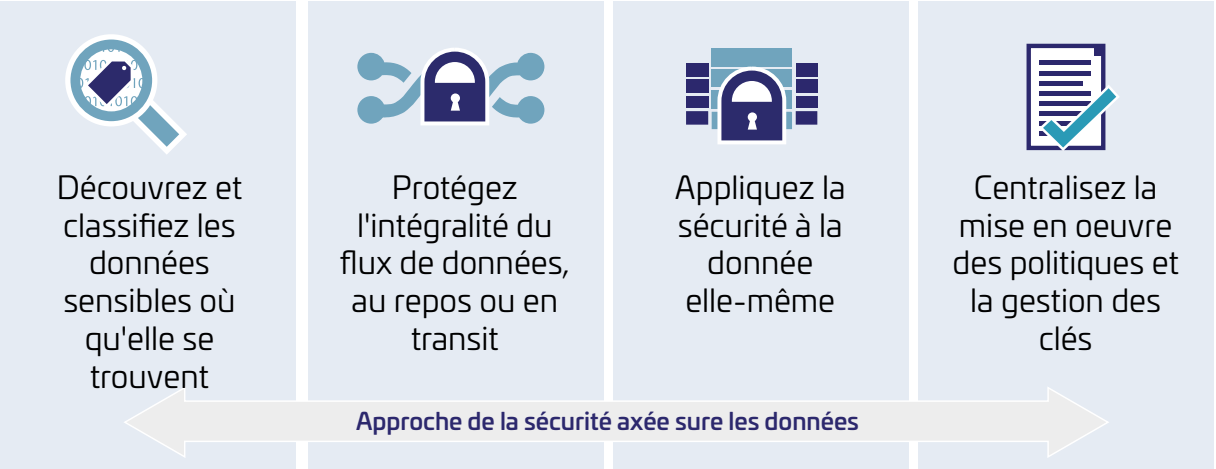
Les fuites de données engendrent des répercussions importantes, allant de la perte de clients à des amendes pour infraction à un règlement ou des coûts de réparation. La défense contre les menaces informatiques est une tâche colossale, personne ne prétend le contraire. Les données et actifs des entreprises, gouvernement et individus sont constamment menacés par une série de nouvelles menaces portant sur la sécurité des données, comme les programmes malveillants, le phishing, le machine learning, les cryptomonnaies et bien d'autres.

Comment faire face à ces défis relatifs à la sécurité des données

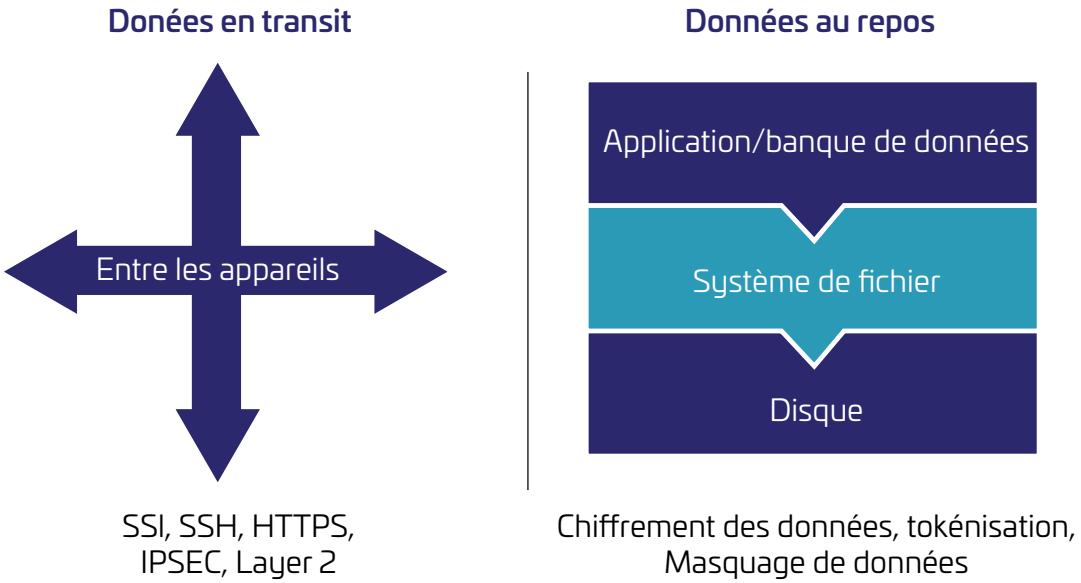
Près de l'ensemble des règlements et normes de conformité existants dans le monde repose sur une approche de la sécurité axée sur les données : il s'agit des meilleures pratiques de base. La sécurité axée sur les données est avant tout définie par une protection appliquée directement aux données, indépendamment de leur emplacement.

Malheureusement, la plupart des technologies de sécurité des données apportent avant tout une protection à l'endroit où se trouve la donnée (ordinateur, serveur ou machine virtuelle dans le cloud spécifique) au lieu de protéger par le biais du chiffrement ou de la tokénisation la donnée elle-même. Le problème lié à cette approche est que dès que les données sensibles sont déplacées ailleurs, il est nécessaire d'avoir recours à une autre solution. Cela conduit à une multiplication des produits de sécurité des données nécessaires pour chaque silo de données.

La sécurité axée sur les données, au contraire, se concentre sur ce qui doit être protégé : les fichiers contenant des informations sensibles. Cette approche applique la forme de protection la plus adaptée, quel que soit l'endroit où se trouvent les données. Pour que cette approche soit efficace, elle doit être automatique. Les informations sensibles doivent être identifiées comme telles dès qu'elles entrent dans l'écosystème informatique de l'organisation et doivent être protégées grâce à une protection reposant sur une politique qui durera tout le long du cycle de vie des données.



Les données peuvent être exposées à des risques lorsqu'elles sont en transit comme au repos et doivent donc être protégées dans les deux états. Il existe de nombreuses approches à la protection des données en transit et au repos. Le chiffrement joue un rôle clé dans la sécurité des données et constitue un outil populaire pour la protection des données, qu'elles soient en transit ou au repos. Lorsqu'il s'agit de protéger les données en transit, les entreprises choisissent souvent de chiffrer les données sensibles avant de les déplacer et/ou utilisent des dispositifs de chiffrement réseau pour protéger le contenu de ces données. Dans le cas de la protection de données au repos, les entreprises peuvent choisir de chiffrer les données sensibles dans des fichiers et bases de données avant de les stocker et/ou choisir de chiffrer le disque de stockage lui-même.



Dès lors qu'une organisation utilise des technologies de chiffrement pour protéger ses données, la sécurité de l'entreprise dépend de la clé de chiffrement et de la gestion des politiques associées, c'est-à-dire la capacité de générer, distribuer, stocker, alterner et annuler/détruire les clés de chiffrement suivant les besoins pour protéger les informations sensibles auxquelles elles sont associées. Elle doit également adopter les meilleures pratiques en matière de sécurité des données telles que la séparation des tâches entre les administrateurs des clés et les utilisateurs. Les bons systèmes de gestion de clé offrent également la possibilité de tirer parti d'une racine de confiance matérielle pour la création et le stockage de clés.

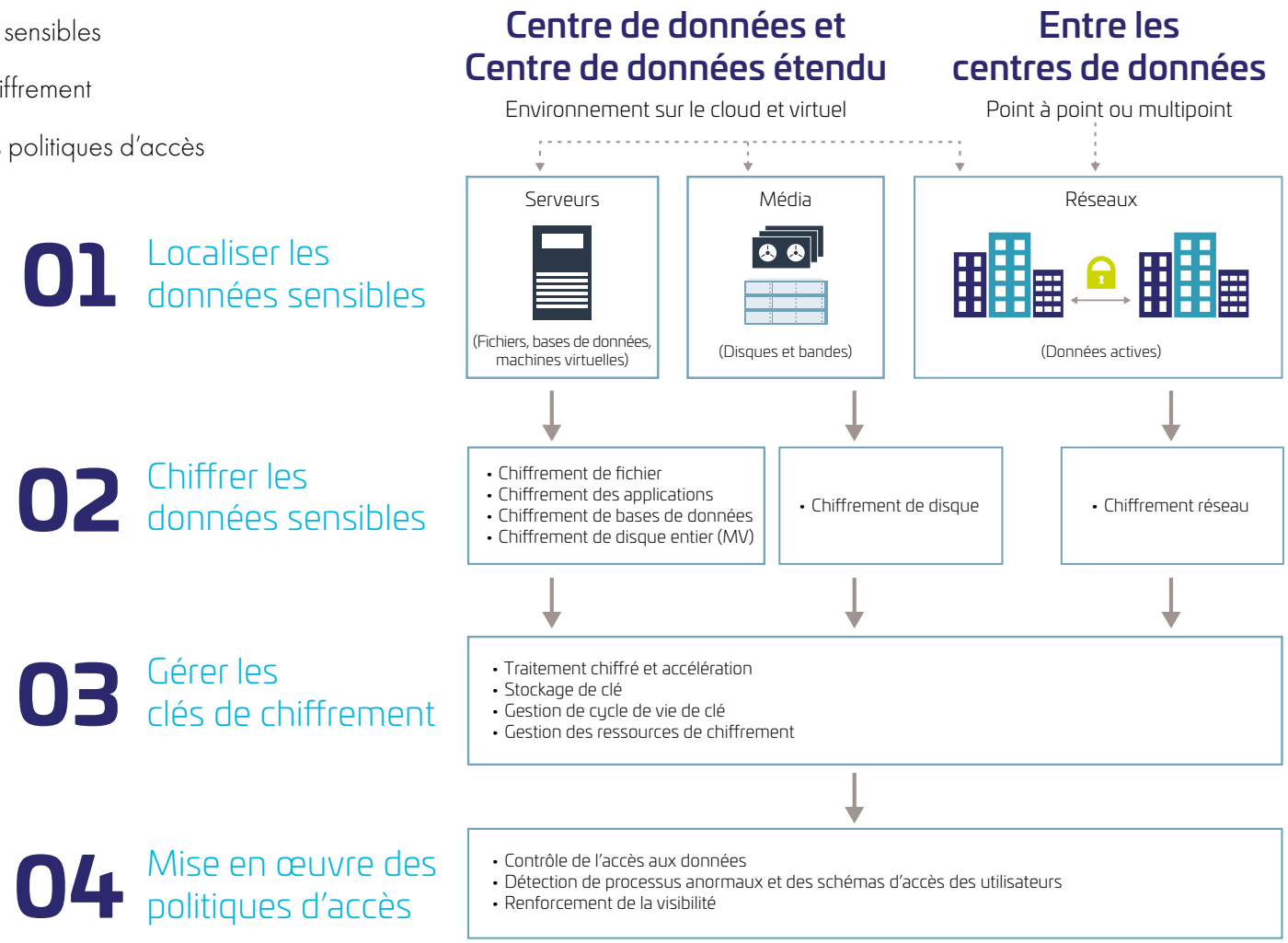
Lorsqu'elle est correctement mise en œuvre, la sécurité axée sur les données offre à l'organisation un contrôle total de ses données sensibles à partir du moment où chaque fichier ou enregistrement de base de données est créé. L'accès aux données protégées peut être accordé ou révoqué à tout moment, et toute activité devrait être enregistrée afin de pouvoir faire l'objet de vérification et de rapport.

L'application correcte de votre approche de sécurité axée sur les données repose sur la prise en compte des méthodes de chiffrement et de protection des données disponibles, et l'audit des accès autorisés et non autorisés aux clés de chiffrement et aux données que vous protégez. Le choix d'un fournisseur disposant de l'éventail de solutions le plus large possible, qui offre une gestion centralisée des clés et des politiques, facilitera le déploiement et les contrôles de gestion lorsque vous augmenterez votre base installée.

Comment aborder la protection des données à l'échelle de l'entreprise ?

Il existe quatre étapes communes à suivre lorsqu'on aborde la protection des données à l'échelle de l'entreprise :

1. Découvrir et classifier les données sensibles
2. Chiffrer les données sensibles
3. Gérer les clés de chiffrement
4. Mettre en œuvre les politiques d'accès



Commencez par identifier l'emplacement de vos données les plus sensibles dans votre centre de données sur site, puis passez à votre centre de données étendu (cloud et environnements virtuels). Effectuez des recherches sur vos serveurs de stockage et de fichiers, vos applications, vos bases de données et vos machines virtuelles. Ne négligez pas le trafic qui circule sur votre réseau et entre les centres de données. Une fois que ces données sortent des limites de votre organisation, vous ne les contrôlez plus.

Ensuite, utilisez une solution de sécurité axée sur les données pour les chiffrer. Heureusement, les solutions pour les entreprises actuelles offrent déjà la technologie permettant de chiffrer les données à l'échelle, et de manière centralisée sans perturber le flux de votre activité.

Et n'oubliez pas les clés. En gérant et en stockant vos clés de manière centralisée, tout en les séparant des données, vous pouvez conserver la propriété et le contrôle et rationaliser votre infrastructure de chiffrement à des fins de vérification et de contrôle.

Une sécurité efficace des données peut être un atout concurrentiel essentiel pour les entreprises numériques d'aujourd'hui. Les données sont au cœur de presque toutes les organisations. Pouvoir les protéger tout en en facilitant l'utilisation efficace pour accroître la valeur de l'entreprise constitue un facteur clé de réussite.

Qu'est-ce qu'une sécurité efficace des données ?

Les meilleures solutions relatives à la sécurité des données fourniront un ensemble intégré de capacités de protection des données, qui permettront aux organisations d'être plus visibles, d'utiliser des renseignements utiles, d'appliquer des contrôles en temps réel et d'automatiser la conformité tout au long du processus de protection des données. Certaines des capacités essentielles de protection des données se trouvent dans le diagramme ci-dessous :

Découverte de données

La découverte de données consiste à obtenir des informations exploitables en repérant des schémas dans les données provenant de sources multiples, grâce à une analyse visuelle interactive. Le terme "Data Discovery" est utilisé pour exprimer un mode d'analyse grâce auquel les utilisateurs tentent d'obtenir une vue globale de toutes leurs sources de données, de déterminer où les données résident et de découvrir les bases de données ou les sources de fichiers de leur réseau qui contiennent potentiellement des données sensibles ou réglementées.

Classification des données

La classification des données est définie au sens large comme le processus d'organisation des données par catégories pertinentes afin qu'elles puissent être utilisées et protégées plus efficacement. Il s'agit d'analyser les différentes sources de données découvertes pour identifier le type de données contenues, et de les associer à un jeu prédéfini de schémas et de mots clés. Il faut ensuite attribuer des étiquettes suivant le type de données pour aider à développer les politiques. La classification des données est particulièrement importante pour la gestion des risques, la conformité et la sécurité des données.

Camouflage des données

Au cœur de la protection des données axée sur les données se trouve le principe selon lequel les données disposent de leur propre défense. Cette défense est rendue possible en rendant les données inintelligibles sans les outils nécessaires pour les déchiffrer, puis en isolant ces outils des données et en contrôlant soigneusement l'accès aux outils. Le chiffrement et la tokénisation font partie des moyens de rendre les données inintelligibles, et la gestion de clé est le processus qui consiste à isoler et à protéger les outils nécessaires pour rendre les données à nouveau intelligibles.

Gestion de clé

La gestion de clé de chiffrement consiste à gérer le cycle de vie complet des clés cryptographiques et à les protéger contre la perte ou l'utilisation abusive. Le cycle de vie comprend : la génération, l'utilisation, le stockage, l'archivage et la suppression des clés. La protection des clés de chiffrement comprend la limitation de l'accès aux clés (physiquement et par l'accès des utilisateurs/rôles), la distribution sécurisée des clés à travers des paysages de chiffrement complexes, la centralisation de la gestion de clé et la mise en place d'une gestion de clé organisée et sécurisée qui maintient les données privées et conformes (FIPS).

Chiffrement

Le chiffrement des données traduit les données sous une autre forme, ou code, de sorte que seules les personnes ayant accès à une clé secrète (formellement appelée clé de déchiffrement) ou à un mot de passe peuvent la lire. Les données chiffrées sont communément appelées ciphertext, tandis que les données non chiffrées sont appelées texte en clair. Actuellement, le chiffrement est l'une des méthodes de sécurité des données les plus populaires et les plus efficaces utilisées par les organisations. Il existe deux principaux types de chiffrement des données : le chiffrement asymétrique, également connu sous le nom de chiffrement à clé publique, et le chiffrement symétrique.

Tokénisation

La tokénisation est le processus qui consiste à transformer une donnée significative, telle qu'un numéro de compte, en une chaîne de caractères aléatoire appelée token qui n'a aucune valeur significative en cas de brèche. Les tokens servent de référence aux données originales, mais ne peuvent pas être utilisés pour deviner ces valeurs. C'est parce que, contrairement au chiffrement, la tokénisation n'utilise pas un processus mathématique pour transformer les informations sensibles en tokens.

Sécurité du cloud

Une solution de chiffrement adéquate doit vous permettre de garder le contrôle et la propriété de vos données et de vos clés de chiffrement non seulement sur site, mais aussi dans un cloud public et dans les environnements hybrides et virtuels. La sécurité du cloud varie considérablement en fonction du fournisseur de cloud et du modèle de déploiement que vous choisissez. D'une manière générale, il existe trois options, comme indiqué ci-dessous :

- **Apportez votre propre chiffrement et gestion centralisée des clés :** cela vous permet de sécuriser vos données sensibles dans votre monde hybride avec un maximum de contrôle, de visibilité et de portabilité. Cette option n'est liée à aucun cloud, fournisseur ou emplacement, ce qui vous offre la possibilité d'unifier la sécurité pour bénéficier d'une simplicité opérationnelle et assurer la conformité.
- **Les services de chiffrement du cloud suivant la technologie Bring Your Own Key :** afin de se conformer aux meilleures pratiques en matière de gestion de clé de chiffrement, la plupart des fournisseurs traditionnels de IaaS/PaaS offrent des interfaces de programmation d'application (API) avec la technologie Bring Your Own Key (BYOK), et certains offrent une solution Hold Your Own Key (HYOK). Dans un environnement multi-cloud avec leur propre technologie BYOK et API, il est probable que vous deviez ajouter des outils pour gérer les clés de chiffrement BYOK.
- **L'utilisation de services de chiffrement natifs :** ceux-ci sont propres à un fournisseur de services de cloud et entièrement gérés par lui. En fonction de votre profil de risque et de la sensibilité des données, vous devrez peut-être compléter ces services par des outils supplémentaires de visibilité, de contrôle et de portabilité.

La stratégie du chiffrement intégral

Comme nous l'avons déjà souligné, les risques et menaces internes comme externes qui pèsent sur vos informations sont de plus en plus importants sur le plan de la portée, du volume et de l'impact. Ainsi, alors que votre organisation est soumise à une pression croissante pour rester compétitive et se conformer aux nouvelles réglementations, le but final est de protéger les données de l'organisation. La protection de l'entreprise numérique dépasse une simple protection contre les cyber-menaces : elle inclut également la confidentialité, l'intégrité et la disponibilité de vos données.

Bien qu'aucune organisation ne soit à l'abri des menaces de brèches de sécurité, la mise en œuvre du chiffrement des données est une garantie majeure qui protégera les actifs et la réputation de votre organisation. La plupart des organisations s'accordent à dire que le chiffrement des données sensibles, en particulier des données au repos, est une stratégie de protection des données fiable. Mais ce raisonnement comprend une erreur.

Premièrement, les données sont plus nombreuses que jamais auparavant, et elles continuent d'être créées à un rythme vertigineux. On présume souvent que le chiffrement est un processus pénible, et il est donc limité aux informations les plus précieuses. Ce qui conduit à des problèmes de classification de données. Sans classification des données, vous ne savez pas où se trouvent ces données sensibles, ce qui interagit avec elles, ni ce que ces données représentent pour votre organisation en termes de valeur et de risque clé. Mais qu'entend-on par « sensible » ? Tout le monde ne s'accorde pas sur la définition du terme « sensible » : les organisations dépensent donc beaucoup de temps et d'énergie à le définir. Il faut beaucoup de temps et de ressources pour mettre cela en application.

Ce n'est plus le cas. Par le passé, le chiffrement omniprésent a largement été abandonné car il coûtait trop en termes de temps, de ressources de calculs, d'espace, d'efficience opérationnelle, de gestion et de facilité d'utilisation générale. Ces défis techniques ont conduit à la pratique de ne chiffrer que les données sensibles. Cependant, l'intégralité ou presque de ces obstacles ont été supprimé et résolus, ouvrant la voie à une stratégie rentable et simplifiée du chiffrement intégral pour les responsables de la sécurité.

Le chiffrement de toutes vos données vous garantit de toujours être en conformité avec les diverses normes et exigences réglementaires, à mesure que les données circulent dans l'entreprise et même entre les différents sites et dans le cloud. Tout aussi important, une approche qui consiste à tout chiffrer peut protéger la marque et la réputation de votre organisation. La plupart des experts s'accordent à dire que presque toutes les organisations seront victimes d'une fuite de données à un moment ou un autre : la question n'est pas de savoir « si » vous serez attaqué, mais « quand » cela arrivera. Imaginez la tranquillité d'esprit (et la réduction de risques) qui accompagnerait la certitude que toute donnée volée à votre organisation est chiffrée et donc sans valeur pour le cybercriminel qui est responsable. La plupart des standards de conformité stipulent que si vos données sont chiffrées, il n'est pas nécessaire de signaler publiquement les failles de sécurité concernant des données. Vos pairs qui s'en tiennent à une approche de chiffrement uniquement centrée sur les données sensibles devront passer plusieurs cycles à déterminer si les données volées étaient sensibles, et si elles étaient chiffrées. Si ce n'est pas le cas, ils devront signaler publiquement la brèche. Les dommages s'étendront à la marque et à la réputation de l'entreprise aux yeux des clients, des partenaires, des employés potentiels et des autres parties prenantes.

Des personnes très intelligentes dans des entreprises tout aussi intelligentes sont arrivées à la conclusion que le chiffrement d'une grande majorité de leurs données est l'une des meilleures options pour réduire les risques et apaiser les craintes de leurs clients. Bien qu'aucune entreprise ou qu'aucun PDG ne souhaite parler de brèche de données, disposer d'une stratégie globale pour faire de la protection des données une priorité est une bonne décision, tant du point de vue de la sécurité que du marketing.

Une stratégie du chiffrement intégral garantit le chiffrement de toutes les données et leur protection par des contrôles d'accès stricts, de sorte que seules les personnes ayant besoin de l'accès à ces données pour des raisons professionnelles ont accès à ces données et uniquement à celles-ci. Et les responsables de la sécurité sont en mesure d'évaluer les différents risques en maintenant, modélisant et offrant l'accès aux données de façon totalement différente et nouvelle.

Comment Thales vous aide à sécuriser vos données

Thales offre les solutions dont vous avez besoin pour protéger vos données sensibles au repos et en transit, même en cas de brèche. Grâce à Thales, vous pouvez appliquer la protection des données là où vous en avez besoin, quand vous en avez besoin et comment vous en avez besoin, en respectant les besoins uniques de votre entreprise.

Les entreprises, gouvernements et organisations font confiance à Thales pour protéger leurs données les plus sensibles. Nos solutions avancées de découverte et classification des données, de chiffrement, de gestion de clé, de tokénisation et de HSM permettent aux clients de sécuriser les paiements numériques, d'être en conformité avec les réglementations en vigueur et de protéger et garder le contrôle de leurs données où qu'elles se trouvent : cloud, centres de données, réseaux et environnements informatiques hybrides.

Comme décrit ci-dessus, il existe de nombreuses techniques et méthodes qui peuvent être utilisées pour déployer une stratégie de chiffrement intégral, et il n'existe peut-être pas de technique universelle, mais le fait de disposer des options disponibles sur une seule plateforme vous permet de sécuriser plus facilement vos données aujourd'hui et à l'avenir.

Les meilleures solutions relatives à la sécurité des données de Thales

La gamme de solutions relatives à la sécurité des données au repos de Thales offre une protection inégalée : elle sécurise les bases de données, les applications, les serveurs de fichiers et le stockage sur site, sur le cloud et dans les environnements virtuels. La plateforme CipherTrust Data Security Platform unifie la découverte, la classification et la protection des données avec des contrôles d'accès granulaires uniques et une gestion centralisée des clés, le tout sur une unique plateforme. Cela vous permet de réduire les ressources dédiées aux opérations de sécurité des données et aux contrôles de conformité omniprésents et de diminuer considérablement les risques pour votre entreprise.

Afin de protéger les clés, nos HSM d'utilisation générale, de paiement et cloud, leaders sur le marché, offrent la confiance nécessaire pour protéger les fonctions et infrastructures de chiffrement des organisations internationales les plus préoccupées par leur sécurité.

En plus de ses solutions de sécurité des données qu repos, Thales propose la gamme de dispositifs de chiffrement réseau à haute vitesse High Speed Network Encryptors pour protéger les données sensibles lorsqu'elles circulent sur les réseaux à des vitesses allant jusqu'à 10 Gb/s.

Cette approche holistique signifie que vous pouvez répondre dès maintenant à vos besoins immédiats en matière de protection des données, tout en investissant dans une solution qui offre une sécurité solide, un écosystème en pleine croissance et la capacité d'évolution dont vous avez besoin pour construire un cadre de confiance pour l'avenir.

Résumé

Les organisations qui veulent survivre et prospérer en cette ère de transformation numérique ont besoin de tous les avantages qu'elles peuvent obtenir : les meilleurs talents, les meilleures stratégies et, bien sûr, la meilleure technologie. Après tout, la technologie a contribué à rendre les transactions commerciales plus rapides, plus transparentes et plus efficaces. Le big data, le cloud computing, l'« internet des objets », la robotique, les bots et autres formes d'intelligence artificielle sont autant de technologies que votre organisation envisage ou examine probablement, si elles ne sont pas déjà utilisées.

Ces technologies brouillent ou éliminent également les périmètres traditionnels des entreprises, et présentent de nouveaux canaux pour les cyberattaques, car les attaquants deviennent simultanément plus sophistiqués. Nous vivons dans un monde de logiciels malveillants, de logiciels de rançon, de phishing, de menaces intérieures, d'attaques d'États nations, d'APT, d'injections SQL et d'ingénierie sociale.

Il n'existe pas de solution miracle pour se protéger contre cette réalité, mais si les responsables de la sécurité des systèmes d'information « remontent la trace de l'argent » et se concentrent sur une approche de la protection des données du chiffrement intégral, ils peuvent devenir des facilitateurs pour de nouvelles utilisations commerciales et technologiques tout en protégeant les données qui leur sont confiées par les parties prenantes, ainsi que la réputation et la solidité financière des organisations qu'ils servent.

Avec les solutions de protection des données de Thales, vous pouvez gérer de manière rentable et efficace la sécurité des données au repos et en transit dans toute votre organisation.

THALES

Contactez-nous

Retrouvez les coordonnées de nos bureaux sur notre site internet cpl.thalesgroup.com/fr/contact-us

> cpl.thalesgroup.com <