cpl.thalesgroup.com

THALES

Les principaux piliers de la protection des données sensibles dans toutes les entreprises

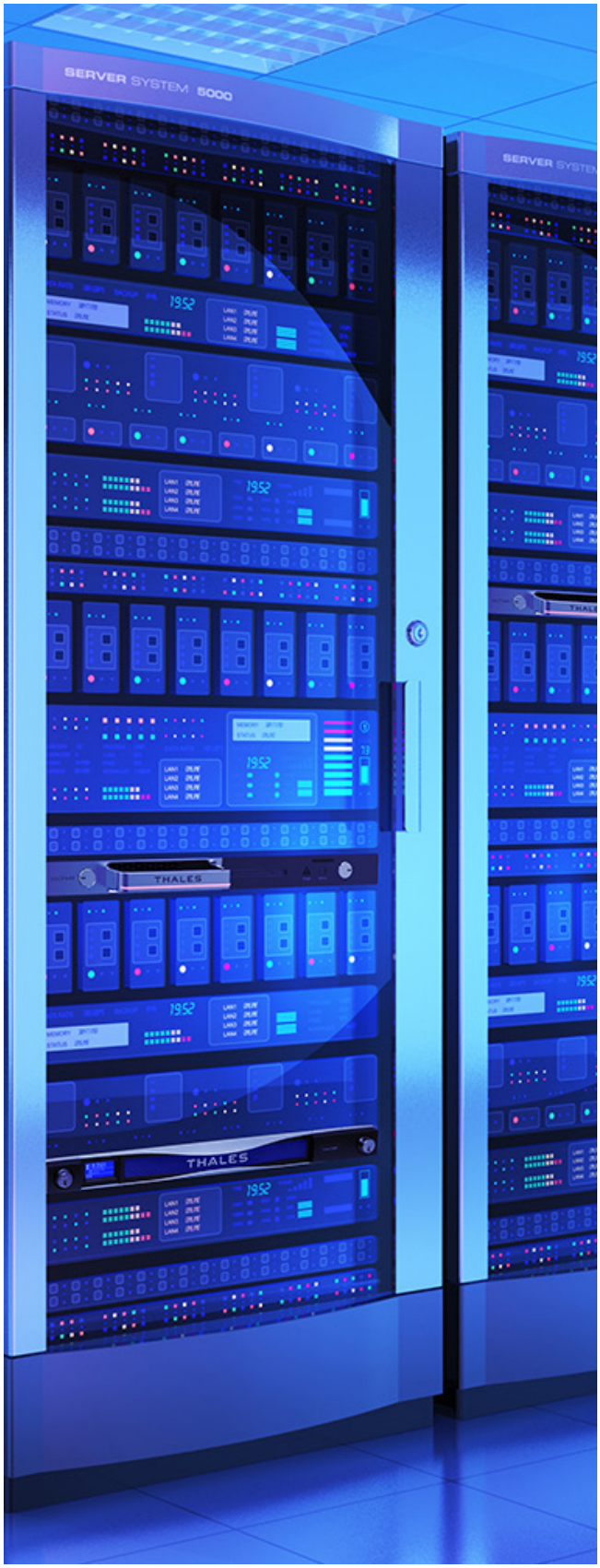
Livre blanc

Table des matières

Introduction

Traditionnellement, les entreprises concentrent principalement leur sécurité informatique sur la défense de leur périmètre, construisant des murs pour empêcher les menaces externes de s'introduire dans le réseau. C'est une mesure importante, mais elle ne suffit pas. Les cybercriminels pénètrent souvent les défenses des périmètres, et les données résident souvent hors de ces périmètres, dans un cloud externe par exemple. C'est pourquoi les entreprises doivent appliquer une stratégie de sécurité axée sur les données qui protège ces dernières où qu'elles se trouvent. Avec la prolifération des données, l'évolution des règles locales et mondiales relatives à la protection des données personnelles, l'adoption croissante du cloud et la persistance des menaces avancées, la sécurité axée sur les données permet aux entreprises de garder le contrôle de leurs données quel que soit leur emplacement tout en les rendant illisibles pour les voleurs de données. Cependant, pour être efficace, cette protection doit être automatique et ne pas reposer sur une intervention de l'utilisateur.

Ce livre blanc présente les défis de la sécurité des données à l'ère de la prolifération des données. Il offre également des stratégies de découverte et de classification de vos données essentielles, ainsi que d'application d'une sécurité axée sur les données afin de les protéger.



Prolifération des données, augmentation des réglementations et cybercriminels plus compétents

Auparavant, de nombreuses architectures de sécurité des données ont été construites sur la supposition que les données seraient actives dans un centre de données et consommées sur site. L'environnement informatique traditionnel était contrôlé par l'IT du début à la fin. L'IT contrôlait et opérait l'infrastructure, la sécurité et les applications. Elle avait donc une immense visibilité et un grand contrôle sur les données et les utilisateurs. Tous les accès aux données et aux applications traversaient des couches de sécurité du périmètre, comme des pare-feux, des pare-feux de nouvelle génération, des VPN, des anti-virus, un système de prévention des intrusions, etc.

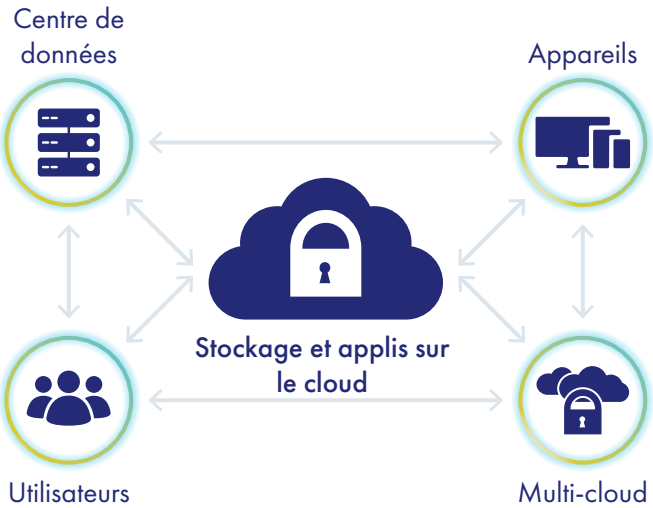
Déplacer la sécurité au-delà du périmètre pour protéger ce qui compte vraiment

Anciennes architectures de sécurité de données

Pas de confiance

Sécurité basée sur un périmètre de confiance

Architecture de sécurité axée sur les données



La sécurité protège les données partout

Toutefois, pour les entreprises modernes, ces mesures ne sont plus pertinentes. Quelle que soit la résistance du périmètre qui entoure le centre de données, la sécurité offerte n'est que conceptuelle, car :

1. La sécurité du périmètre ne peut pas s'adapter au mouvement et à la prolifération des données

L'adoption généralisée des services cloud, des environnements Big Data et des technologies IoT signifie que les entreprises doivent gérer un énorme volume de données très rapidement, souvent avec la difficulté supplémentaire que représentent les infrastructures tierces et les partenaires. Ceci engendre de nombreuses difficultés :

- Diverses formes de données, dont des données structurées, semi-structurées et non-structurées
- Goulots d'étranglement de la sécurité du périmètre qui génèrent de la latence et un ralentissement des performances qui violent les accords de service (SLA), c'est pourquoi les utilisateurs ont souvent un accès direct aux services du cloud.
- Les "initiés" sont partout : les initiés ne sont plus vos employés dans votre périmètre. Vos données sont aujourd'hui entre les mains de sous-traitants, de fournisseurs de service et d'autres tiers. Ces « initiés » sont des individus que vous n'avez pas approuvés, que vous ne pouvez pas surveiller et que vous ne contrôlez pas.

2. Complexité opérationnelle et réglementation

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 entreprises doivent redoubler d'effort pour payer des politiques unifiées et cohérentes, ainsi que pour les appliquer, les gérer et les distribuer aux différentes ressources informatiques. Chaque entreprise dispose d'un mélange de plateformes nouvelles et anciennes.

En parallèle de la croissance exponentielle des données, les règles mondiales et locales relatives à la protection des données personnelles sont de plus en plus nombreuses et multiplient les exigences de conformité. Pour respecter ces exigences et protéger leurs données, les entreprises ne peuvent plus se fier à des approches anciennes et compartimentées.

Tout ceci complexifie énormément les environnements de données actuels. Le fait que les entreprises perçoivent la complexité opérationnelle comme l'obstacle principal au déploiement de la sécurité des données n'est donc pas une surprise. Les directeurs de la sécurité informatique (CISO) et les directeurs de systèmes de données (CDO) sont de plus en plus nombreux à reconnaître le besoin de solutions de sécurité des données intégrées qui fournissent une protection solide pour les données sensibles, où qu'elles soient stockées ou utilisées.

Étant donné que les architectures de la sécurité des données héritées ne prennent pas en compte de nombreuses caractéristiques du monde moderne axé sur les données, elles ne peuvent pas protéger les entreprises contre les brèches de données sophistiquées engendrées par des assaillants toujours plus déterminés. Aujourd'hui, si les CISO et les CDO souhaitent sortir du cercle vicieux de mesures et de contre-mesures, ils doivent adopter une approche totalement différente.

La complexité opérationnelle est l'obstacle principal au déploiement de la sécurité des données

Stratégie de protection des données sensibles dans votre entreprise en trois points

Les architectures de sécurité héritées ont souvent montré leurs limites de manière spectaculaire, car elles sont adaptées à un mode d'interaction archaïque entre les entreprises et leurs données. Aujourd'hui, la sécurité des données doit reconnaître non seulement que les données sont l'actif le plus important d'une entreprise, mais également qu'elles prolifèrent de manière exponentielle.

La sécurité axée sur les données protège les données elles-mêmes au lieu des points de terminaison, des réseaux et des applications entre lesquelles elles circulent. Les données elles-mêmes sont protégées, ce qui leur permet de s'adapter aux évolutions de l'entreprise sans aucun risque. Au lieu de ralentir les progrès et de limiter la prolifération des données, la sécurité axée sur les données permet à l'entreprise de tirer le maximum de ses données, où qu'elles soient stockées et utilisées.

Ce graphique montre les trois piliers principaux de la sécurité axée sur les données.

Les trois piliers de la sécurité des données

Nº 1
Découverte et classification des données sensibles

- Découvrir et classifier de manière efficace les données sensibles
- Bien comprendre les données et leurs risques

Nº 2
Protection des données sensibles

- Protéger les données sensibles avec le chiffrement, le contrôle des accès et la tokénisation
- Ceci permet de les rendre illisibles et inutiles en cas de vol ou de fuite

Nº 3
Contrôle des clés de chiffrement

- Gestion centralisée des clés
- Gestion du cycle de vie des clés
- Politiques unifiées de chiffrement et de gestion de clé

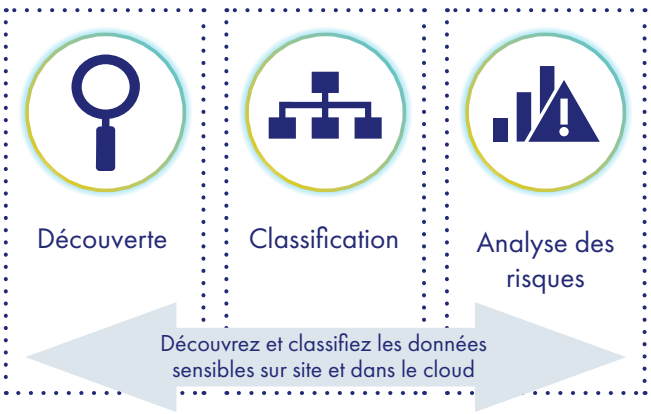
Une approche de la sécurité axée sur les données doit être intégrée à l'ADN de l'entreprise. Cette approche globale est basée sur l'expérience de Thales qui a travaillé avec des centaines de CISO, de CDO, de PDG et d'architectes de nombreuses entreprises qui sont au plus près de la sécurité et de la protection des données, ainsi que sur les meilleures pratiques exigées par de nombreuses réglementations et normes de l'industrie. Pour adopter cette approche de la sécurité des données, les entreprises doivent :

1. Découvrir et classifier les données sensibles

Les données sensibles sont partout dans l'entreprise, dans le cloud et au-delà. En général, l'équipe de sécurité IT a peu de visibilité sur les sites de stockage des données et sur qui y a accès. Il y a plusieurs risques, dont les brèches et les violations de conformité. Commencez par identifier l'emplacement de vos données les plus sensibles dans votre centre de données sur site, puis passez à vos environnements étendus, comme le cloud et les services hébergés. Effectuez en premier lieu des recherches sur vos serveurs de stockage et de fichiers, vos applications, vos bases de données et vos machines virtuelles. Trouvez les données dans votre entreprise où qu'elles soient et classifiez-les selon leur sensibilité et leur importance en fonction des politiques internes et des réglementations externes.

Découvrir, identifier et classifier vos données sensibles est la première étape du processus, mais il faut pouvoir la répéter et ce, indépendamment de la technologie ou de la géographie. Les solutions actuelles de découverte et de classification des données fournissent des tableaux de bord et des listes qui vous aident à bien comprendre le type de données sensibles dont vous disposez, où elles sont situées et leur score de risque. Les scores de risque prennent en compte plusieurs paramètres tels que le niveau de protection, le nombre d'éléments découverts, leur emplacement, le volume de données sensibles, etc., ce qui permet aux entreprises d'identifier la sensibilité des objets de données comme les fichiers et les bases de données. Les entreprises peuvent ensuite protéger les données et limiter les risques, par exemple en hiérarchisant la remédiation ou en prenant des décisions éclairées sur le partage de données avec des tiers ou la migration dans le cloud.

La découverte et la classification des données est la première étape d'une sécurité des données efficace



2. Protéger leurs données sensibles

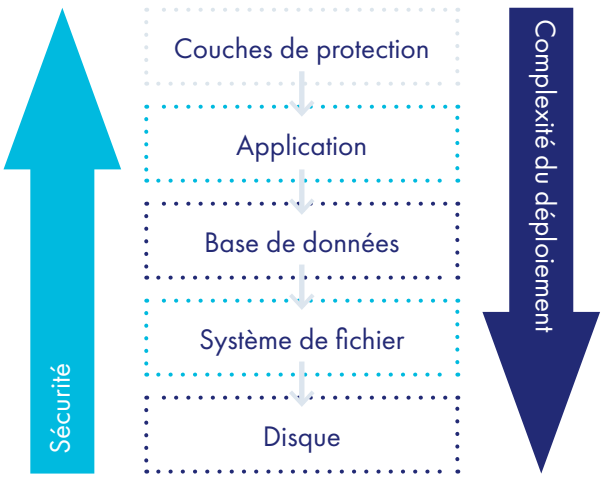
Idéalement, pour protéger les données sensibles elles-mêmes, il vous suffit de définir une stratégie de chiffrement de base pour toute votre entreprise, qui permet de limiter les risques de fuite et de brèche de données.

Une fois vos données découvertes et classifiées, vous pouvez déterminer le risque lié à chaque ensemble de données pour votre entreprise et évaluer où mettre en place en priorité des mécanismes de sécurité de camouflage et de contrôle d'accès, tels que le chiffrement au niveau du fichier avec des contrôles d'accès granulaires et la tokénisation avec le masquage de données dynamique. Ceci revient à protéger les données en rendant l'accès par des utilisateurs non autorisés plus difficile et en les rendant illisibles et inutiles en cas de vol ou de fuite.

Actuellement, le chiffrement est l'une des méthodes de sécurité des données les plus populaires et les plus efficaces utilisées par les entreprises. Le chiffrement des données transforme les données et les rend illisibles de manière à ce que seuls les utilisateurs autorisés puissent accéder aux données sous forme de texte lisible. Le chiffrement transforme les données à l'aide d'un algorithme spécifique, mais la tokénisation protège les données sensibles en les remplaçant par des données non-sensibles. La tokénisation crée une forme tokénisée des données qui maintient le format des données sources, sans être reconnaissable. Les données tokénisées peuvent également être stockées au même format et à la même taille que les données originales. Stocker les données tokénisées ne demande donc aucune modification dans le schéma ou le processus de la base de données. Si le type de données stockées n'a pas ce type de structure, par exemple des fichiers texte, des PDF, des MP3, etc., la tokénisation n'est pas le mode de camouflage approprié. Dans ce cas, il vaudra mieux lui préférer un chiffrement au niveau du système de fichier. Ce mode transforme le bloc de données en version chiffrée des données.

Pour déterminer quelle solution de chiffrement des données s'adapte le mieux à votre cas, vous devez prendre en compte plusieurs facteurs. À haut niveau, les types de chiffrement des données peuvent être classés selon l'endroit où ils sont employés dans la pile technologique. Le chiffrement des données est généralement employé sur l'un de ces quatre niveaux : disque, système de fichier, base de données et application. En général, plus le chiffrement est employé en bas de la pile, plus la mise en place est simple et moins elle est intrusive. Cependant, le nombre et le type de menaces que ces approches peuvent contrer est plus limité. D'autre part, en utilisant le chiffrement plus haut dans la pile, les entreprises peuvent atteindre un niveau de sécurité plus élevé et contrer plus de menaces.

La sécurité augmente, mais la complexité du développement augmente également lorsque les mesures de chiffrement sont mises en place plus haut dans la pile



3. Contrôler leurs clés de chiffrement

La sécurité des processus de chiffrement dépend de la sécurité des clés de chiffrement qui servent à chiffrer les données. Si les clés utilisées pour chiffrer ou tokéniser les données sont volées avec les données chiffrées ou tokénisées, les données ne sont pas sécurisées, car elles peuvent être déchiffrées et lues facilement. Pour que le chiffrement et la tokénisation protègent véritablement les données sensibles, les clés de chiffrement elles-mêmes doivent être protégées, gérées et contrôlées par votre entreprise, et pas par un tiers ou un fournisseur de cloud.

À mesure que les entreprises déploient toujours plus de solutions de chiffrement compartimentées, elles doivent gérer des politiques hétérogènes, des niveaux de protection différents, et une augmentation des coûts. Pour sortir de ce labyrinthe, le plus simple est d'adopter un modèle de gestion de clé centralisée. La gestion de clé de chiffrement consiste à gérer le cycle de vie complet des clés de chiffrement et à les protéger contre la perte ou l'utilisation abusive. Les clés ont une durée de vie : elles sont créées, elles sont utilisées, puis elles sont abandonnées. Gérer le cycle de vie des clés inclut la génération, l'utilisation, le stockage, la distribution, l'archivage et la suppression des clés. Voici certains avantages de la gestion de clé centralisée :

- Politiques unifiées de chiffrement et de gestion de clé
- Révocation de clé dans le système entier
- Risque d'erreur humaine réduit dans la définition des permissions d'utilisateurs et administratives
- Disponibilité et évolutivité élevées
- Validation de FIPS 140-2 sécurisée
- Économies grâce à l'automatisation
- Informations d'audit consolidées
- Sauvegarde et récupération simplifiées
- Amélioration de la sécurité grâce à une séparation compréhensive des devoirs

Adoptez une gestion centralisée de vos clés de chiffrement

Avantages d'une sécurité efficace axée sur les données

Avec une solution de sécurité efficace axée sur les données, vous pouvez faire face aux défis de sécurité engendrés par la prolifération des données et l'émergence des réglementations mondiales et locales relatives à la protection des données personnelles et préparer votre entreprise pour un futur plus sûr.

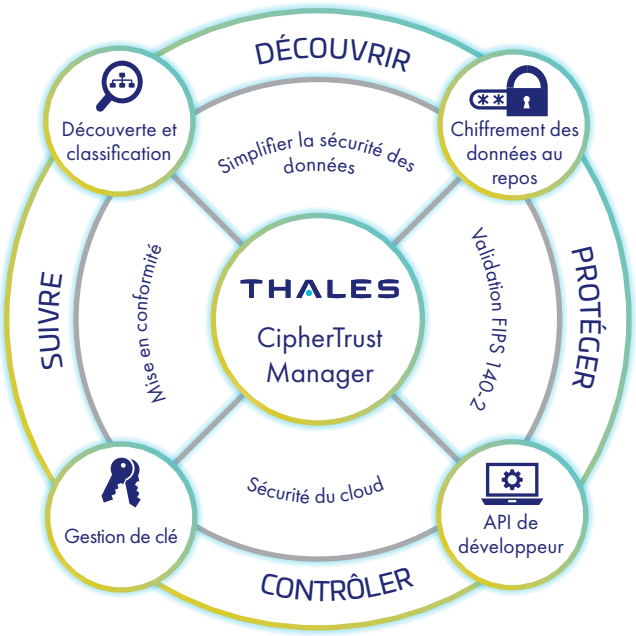
Une solution de sécurité axée sur les données correctement déployée :

- Aide les entreprises à limiter les risques et à réduire les coûts. Les entreprises peuvent réduire les coûts en opérationnalisant l'infrastructure de sécurité existante à grande échelle, en réduisant les processus manuels qui impliquent beaucoup de travail, qui sont répétitifs et qui donnent lieu à beaucoup d'erreurs et en assurant leur investissement sur l'avenir grâce à l'adoption d'une nouvelle technologie.
- Fournit une vue complète et continue de tous les actifs de données et facilite la gouvernance des politiques de sécurité ainsi que le contrôle.
- Aide les entreprises à comprendre leurs données et les risques, et à hiérarchiser la remédiation.
- Protège les données afin qu'elles puissent passer en toute sécurité d'environnements sur site à des environnements sur cloud tout en conservant leur profil de protection.
- Assure la protection des données contre les utilisateurs malveillants et les menaces persistantes avancées qui tentent de voler des informations sensibles.
- Réduit les amendes et aide les entreprises à respecter les réglementations gouvernementales, organisationnelles et de l'industrie. Les entreprises peuvent suivre les infractions et faire appliquer les politiques et les règles de sécurité tout en créant des rapports et des procédures d'audits de sécurité automatisés.
- Crée une position juridiquement défendable en cas de brèche de données ou de problème d'audit.

Comment Thales peut vous aider à mettre en place une stratégie de sécurité en trois points

Thales est le leader mondial de la protection des données Nous fournissons aux entreprises tout ce dont elles ont besoin pour découvrir, protéger et gérer leurs données, leurs identités et leur propriété intellectuelle : découverte et classification des données, chiffrement, gestion de clé avancée, tokénisation et gestion de l'authentification et des accès. CipherTrust Data Security Platform de Thales unifie la découverte des données, la classification, la protection des données avec des contrôles d'accès granulaires inégalés et une gestion centralisée des clés, le tout sur une seule plateforme. Ceci se traduit par une réduction des ressources dédiées aux opérations de sécurité des données, des contrôles de conformité globaux et une réduction significative des risques dans votre entreprise.

CipherTrust Data Security Platform



Capacités clés de la CipherTrust Data Security Platform

- Découverte et classification des données
  - Analyse des risques avec visualisation des données
- Techniques de protection des données
  - Chiffrement transparent pour les fichiers, les bases de données, les Big Data et les conteneurs
  - Protection des données d'application
  - Tokénisation avec masquage de données dynamiques
  - Chiffrement conservateur de format
  - Masquage des données statiques
  - Contrôles d'accès d'utilisateur privilégié
- Gestion centralisée des clés d'entreprise
  - Conformité FIPS 140-2
  - Gestion de clé dans le cloud multiple
  - Écosystème de partenaires d'intégrations KMIP inégalé
  - Gestion de clé de chiffrement de bases de données (Oracle TDE, Big Data, MS SQL, SQL Server Always Encrypted, etc.)
- Surveillance et création de rapports
- Console de gestion centralisée

Avantages de CipherTrust Data Security Platform

Simplifier la sécurité des données

Découvrez, protégez et contrôlez les données sensibles où qu'elles se trouvent avec la protection des données unifiée nouvelle génération. La plateforme CipherTrust Data Security Platform simplifie l'administration de la sécurité des données avec une console de gestion centralisée sur un seul écran pour doter les entreprises d'outils puissants qui permettent de découvrir et de classifier les données sensibles, de combattre les menaces externes, de lutter contre l'abus d'initié et d'établir des contrôles persistants, même quand les données sont stockées dans le cloud ou dans les infrastructures de fournisseurs externes. Les entreprises peuvent facilement découvrir et combler les failles de protection des données, et prendre des décisions éclairées sur les mandats de confidentialité et de sécurité avant la mise en place d'une transformation numérique.

Accélération du processus de mise en conformité

Les régulateurs et les auditeurs ont besoin que l'entreprise contrôle les données sensibles et réglementées dont elle dispose et qu'elle ait des rapports pour le prouver. Les capacités de CipherTrust Data Security Platform, dont la découverte et la classification des données, le chiffrement, les contrôles d'accès, les journaux d'audit, la tokénisation et la gestion des clés, permettent de respecter les exigences en matière de sécurité des données et de confidentialité. Ces contrôles peuvent être rapidement ajoutés à de nouveaux déploiements ou en réponse à une évolution des exigences de conformité. La nature centralisée et extensible de la plateforme permet d'ajouter de nouveaux contrôles rapidement grâce à l'ajout de licences et au déploiement scripté des connecteurs nécessaires en réponse à de nouvelles exigences en matière de protection des données.

Migrations vers le cloud sécurisée

CipherTrust Data Security Platform propose des solutions de chiffrement et de gestion de clé centralisée avancées qui permettent aux entreprises de stocker les données sensibles dans le cloud en toute sécurité. La plateforme propose des solutions multi-cloud avancées de Bring Your Own Encryption (BYOE) permettant d'éviter le verrouillage de chiffrement du distributeur du cloud et d'assurer la mobilité des données pour stocker celles-ci efficacement chez des fournisseurs de cloud multiples grâce à une gestion du chiffrement centralisée et indépendante. Les entreprises ne pouvant pas utiliser les services BYOE (Bring Your Own Encryption) peuvent toujours suivre les meilleures pratiques du secteur en gérant les clés en externe, en utilisant CipherTrust Cloud Key Manager. Le gestionnaire CipherTrust Cloud Key Manager prend en charge les cas d'utilisation BYOK (Bring Your Own Key) sur des infrastructures de cloud multiple et des applications SaaS. Avec CipherTrust Data Security Platform , les protections les plus fortes sont appliquées aux données sensibles et aux applications de l'entreprise dans le cloud, ce qui aide l'entreprise à respecter les exigences de conformité et à mieux contrôler ses données où qu'elles soient créées, utilisées ou stockées.

Réduction du coût total de propriété

CipherTrust Data Security Platform peut réduire le coût total de propriété pour les entreprises de toute taille en simplifiant la sécurité des données, en réduisant les délais de mise en conformité et en assurant la sécurité et le contrôle sur cloud multiple. Construite sur une infrastructure extensible, la plateforme permet à vos départements d'informatique et de sécurité des données de découvrir, classifier et protéger les données inactives dans votre entreprise de manière uniforme et répétable. Utiliser une approche héritée peut souvent s'avérer onéreux et implique l'utilisation de produits spécifiques nécessitant une nouvelle intégration ainsi que de la main d'œuvre supplémentaire pour s'occuper de la gestion, ce qui annule toute économie potentielle. Les nombreux produits disponibles sur CipherTrust Data Security Platform peuvent être déployés de manière indépendante ou en combinaison. Ils préparent votre entreprise à faire face au prochain défi de sécurité ou à la prochaine exigence de conformité pour un coût de propriété minimal. En intégrant la découverte, la classification, l'analyse du risque et la protection des données, le tout sur une seule plateforme, la solution CipherTrust libère le personnel et le budget du département informatique pour des tâches plus stratégiques et favorise une collaboration plus ouverte, dont les entreprises modernes ont besoin, sans sacrifier la sécurité.

Résumé

Les attaques qui ciblent les données sont de plus en plus sophistiquées car les données ont de plus en plus de valeur, et les entreprises doivent protéger leurs informations les plus sensibles et défendre leur réputation. La sécurité axée sur les données est la seule approche qui permet à la fois la mise en conformité et la mise en place d'une protection efficace contre les menaces modernes. Les stratégies de sécurité efficaces axées sur les données basées sur les trois piliers que sont la découverte et la classification, la protection des données et la gestion de clé de chiffrement centralisée permettent aux entreprises d'extraire de la valeur des données sensibles en toute sécurité et d'adopter les technologies de la transformation numérique en toute confiance.

Avec les solutions axées sur les données de Thales, vous pouvez protéger efficacement, et pour un coût réduit, les données sensibles structurées et non structurées dans votre entreprise.

THALES

Nous contacter

Pour savoir où se trouvent nos bureaux ou obtenir nos coordonnées, consultez
cpl.thalesgroup.com/fr/contact-us

> cpl.thalesgroup.com <