

Guide pratique de la sécurité dans le Cloud

Le Trusted Cloud Fabric (Structure Cloud de Confiance) de SafeNet pour conforter votre confiance et maîtriser vos environnements virtualisés.



TRUSTED CLOUD
FABRIC

Guide pratique de la sécurité dans le Cloud

Le Trusted Cloud Fabric (Structure Cloud de Confiance) de SafeNet pour conforter votre confiance et maîtriser vos environnements virtualisés.

Résumé- Pour tirer profit du potentiel stratégique offert par le Cloud, les entreprises doivent relever un défi essentiel : la sécurité. SafeNet permet aux entreprises de relever ce défi avec succès grâce à une série complète de solutions pratiques et concrètes de sécurité auxquelles ont été donné le nom de SafeNet Trusted Cloud Fabric (Structure Cloud de confiance de SafeNet). De l'authentification en environnement SaaS au respect de la conformité dans le Cloud, ces solutions pratiques sont prêtes dès aujourd'hui, vous pouvez les adopter où et quand vous en aurez besoin.

“Forrester prévoit l'émergence de services Cloud hautement sécurisés dans les cinq années à venir. Pendant cette période, la sécurité dans le Cloud évoluera vers un marché de 1,5 milliard de dollars et se transformera passant de frein à facilitateur d'adoption du Cloud.”

—Forrester Research

Introduction

Aujourd'hui, plus de 60% des entreprises, des grands comptes aux petites PME, s'apprêtent à évaluer ou piloter une offre Cloud au cours des 18 prochains mois¹. Pour de nombreuses applications, comme l'automatisation de l'équipe de vente, la gestion de projets et l'automatisation du marketing, l'utilisation du SaaS est devenue de fait la norme. Cependant, au sein de nombreuses entreprises, les premières initiatives Cloud ne représentent qu'une goutte d'eau dans la mer par rapport à ce qui sera finalement mis en place.

Prenons l'exemple d'une importante multinationale dans le commerce de détail. Elle souhaite migrer ses machines virtuelles de l'interne vers le Cloud pendant la période des vacances. 70% de ses activités se déroulant pendant cette période de quatre semaines, cette société devrait pouvoir réduire de manière substantielle ses coûts opérationnels durant les mois de l'année qui enregistrent une demande moins importante, et économiser ainsi des millions.

C'est par la multiplication de ce type d'initiative stratégique que les entreprises vont commencer à se rendre compte de la valeur qu'apporte concrètement le Cloud : flexibilité et réduction des coûts. Néanmoins, pour que ces visions deviennent réalité, il faut relever un défi important : garantir la sécurité, la confiance et la maîtrise du Cloud. Quelles sont les précautions mises en place par les prestataires du Cloud pour se protéger des intrusions? Comment les entreprises peuvent-elles faire en sorte que les données sensibles ne se mélangent par inadvertance aux archives d'un autre client dans un milieu virtuel mutualisé? Comment les entreprises font-elles pour garantir et démontrer la conformité de leurs déploiements Cloud?

Aujourd'hui, les entreprises, du fait du nombre croissant d'initiatives Cloud, se débattent pour trouver des réponses à ces questions. Plus la valeur stratégique des initiatives Cloud augmente, plus les impératifs de sécurité se font urgents et nécessaires. Ce renforcement des demandes sur le plan de la sécurité va entraîner une prolifération des efforts et investissements de la part des entreprises et des prestataires qui les servent dans le domaine de la sécurité. C'est pour cela que Forrester estime que la sécurité dans le Cloud va, d'ici 5 ans, se transformer en un marché représentant 1,5 milliard de dollars².

1 Gartner, "Hype Cycle for Cloud Computing, 2010", David Mitchell Smith, 27 juillet 2010

2 Forrester, "Security And The Cloud: Looking At The Opportunity Beyond The Obstacle", Jonathan Penn with Heidi Shey, Christopher Mines, Chétina Muteba, 20 Octobre 2010

SafeNet Information Lifecycle Protection

Le Trusted Cloud Fabric de SafeNet est une extension de l'approche complète de sécurisation des données à travers tout le cycle de vie de l'information, appelée « Protection du cycle de vie de l'information de SafeNet ». En apportant une plus grande confiance et un meilleur contrôle lors du passage des utilisateurs, données, systèmes et applications à un environnement virtuel, SafeNet permet aux clients d'intégrer efficacement tout modèle Cloud à leurs technologies et stratégies de sécurité à court et long terme.

Chiffrement : Un contrôle fondamental du Cloud

Comme expliqué brièvement lors des paragraphes précédents, avant de migrer des actifs et des services stratégiques sur le Cloud, les organisations doivent être en mesure d'effectuer ce transfert en maintenant les contrôles nécessaires en matière de sécurité. C'est pour cela que les experts de la sécurité et les analystes industriels considèrent de plus en plus que le chiffrement est une nécessité pour les organisations qui adoptent le Cloud. A condition d'être correctement mis en œuvre, et de l'associer aux bonnes approches de gestion des politiques et des clés, le chiffrement permet aux organisations d'isoler les données et les politiques associées, tout particulièrement dans les environnements partagés. Grâce à ces contrôles, les organisations peuvent progresser vers le Cloud, sans compromettre leur sécurité ni leur conformité.

Le chiffrement est une composante critique de la sécurité au sein des datacenters traditionnels et son importance grandit de manière significative dans l'environnement Cloud. Par le passé, des contrôles physiques, des isollements physiques inhérents et plusieurs niveaux sous-jacents de confiance liés aux datacenters réduisaient les besoins potentiels en chiffrement. Avec le Cloud, ces barrières physiques et ces facteurs de confiance ont complètement disparu et le chiffrement est devenu un moyen de contrôle stratégique et essentiel pour avancer.

La solution : Le Trusted Cloud Fabric de SafeNet

SafeNet propose l'offre Cloud la plus complète du marché pour environnements virtualisés, afin de permettre aux entreprises de garantir la confiance tout au long du cycle de vie des données de l'entreprise. Le Trusted Cloud Fabric de SafeNet permet aux entreprises de :

- **Garantir la sécurité et la conformité du Cloud.** Le Trusted Cloud Fabric de SafeNet représente un écosystème complet de solutions de sécurité. Il se compose et relie protection renforcée, chiffrement flexible et souple, garantie d'authentification, ancres de sécurité, et des communications sécurisées. Grâce à toutes ces fonctionnalités, SafeNet permet aux clients de conserver une maîtrise totale sur les activités d'isolement, de protection et de partage de leurs données, même dans des environnements Cloud mutualisés.
- **Suivre un parcours pragmatique pour migrer vers le Cloud.** SafeNet offre une architecture modulaire qui donne aux organisations la flexibilité nécessaire pour évoluer jusqu'au Cloud de la manière la plus efficace et efficiente possible, tout en respectant leurs calendriers spécifiques ainsi que leurs objectifs commerciaux et leurs politiques de sécurité. Le Trusted Cloud Fabric de SafeNet permet aux entreprises de s'attaquer aux défis de sécurité les plus pressants, à court et long terme, qu'elles cherchent à sécuriser l'accès à des applications SaaS, à chiffrer les données stockées dans le Cloud, à protéger les liens de communications entre les Clouds privés et publics ou à atteindre un large éventail d'objectifs.
- **Tirer profit des avantages du Cloud.** Le Trusted Cloud Fabric de SafeNet propose des solutions performantes créées pour soutenir les environnements virtualisés. En outre, les solutions de SafeNet permettent d'obtenir une gouvernance centralisée des données, applications et systèmes sensibles ainsi qu'une gestion centralisée, et ce dans tout le Datacenter et dans tout le Cloud. De ce fait, les équipes chargées de la sécurité peuvent profiter d'une efficacité administrative optimisée alors que l'entreprise adopte totalement les opportunités du Cloud.

Les éléments du Trusted Cloud Fabric

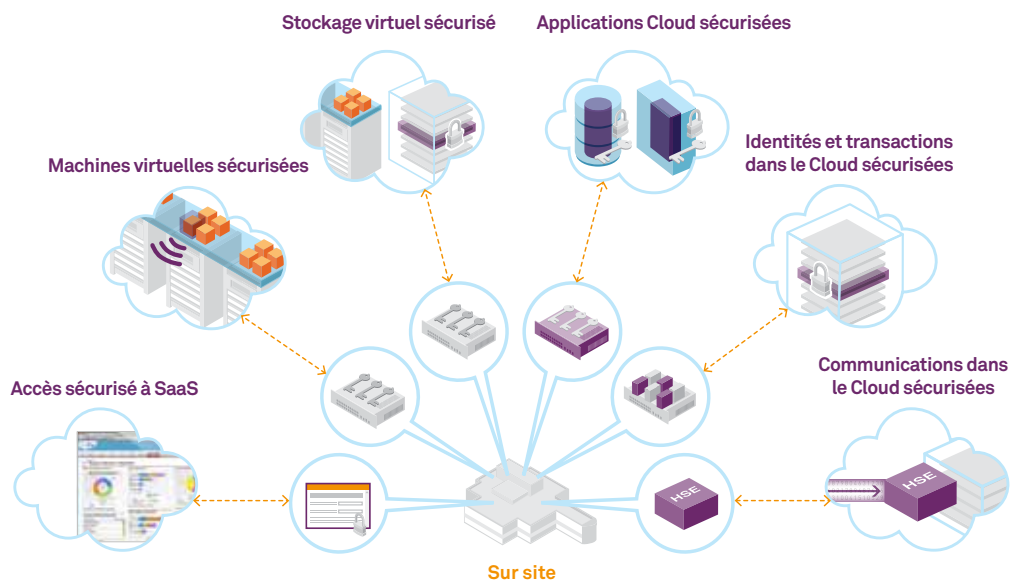
Concernant les initiatives Cloud, on ne peut réduire l'approche à une seule et unique taille, stratégie ou technologie. Chaque entreprise peut suivre sa propre approche et la mener sur plusieurs fronts pour passer au Cloud. Aussi, chaque entreprise a besoin de solutions

Les bénéfices de Trusted Cloud Fabric

- Gardez le contrôle. Conservez la sécurité et le contrôle de vos data centers privés dans votre Cloud public et privé
- Pas de compromis. Renforcez votre sécurité sans compromettre la flexibilité ou l'évolutivité des déploiements vers le Cloud.
- Faites simple. Bénéficiez d'une gestion et d'une administration centralisées et intégrées, dans tous les domaines – incluant les data center internes, et le Cloud public, privé et hybride.
- Inscrivez votre sécurité dans la durée. Profitez d'une protection des informations sensibles à travers tout son cycle de vie, et quelque soit leur emplacement.

modulaires offrant de la flexibilité dans les points d'intégration entre les Clouds publics, privés et hybrides. SafeNet fournit une panoplie complète de solutions afin de proposer aux organisations les fonctionnalités dont elles ont besoin, lorsqu'elles en ont besoin, et adaptées au stade qu'elles ont atteint dans leur stratégie d'adoption de Cloud. SafeNet propose ces solutions basées sur Cloud :

- un accès sécurisé au SaaS
- des identités et transactions sécurisées pour le Cloud
- des instances virtuelles sécurisées
- du stockage sécurisé pour le Cloud
- des données d'applications sécurisées pour le Cloud
- des connexions sécurisées pour le Cloud



Lorsque des organisations migrent vers des environnements de données sensibles ou régulées par des mandats, elles auront probablement à répondre à des questions difficiles: Comment faire pour maintenir l'isolement et la sécurisation des informations dans des environnements mutualisés et distants alors que de nombreux contrôles sécuritaires traditionnels ne peuvent pas être employés. Comment faire pour se protéger contre les copies illimitées d'instances virtuelles ? Comment obtenir la visibilité fondamentale requise pour bien comprendre le mode d'utilisation des instances virtuelles ? Comment faire respecter la séparation des rôles et des contrôles granulaires requis pour minimiser la menace d'emploi abusif des privilèges de super-utilisateurs dont disposent les administrateurs Cloud ?

Pour résoudre ces problèmes, les organisations doivent sauvegarder les instances virtuelles et les actifs sensibles qu'ils contiennent. Les organisations doivent conserver les contrôles de sécurité nécessaires afin que seuls les utilisateurs autorisés puissent accéder aux données sensibles que détiennent, à tout moment, les instances virtuelles. C'est pour toutes ces raisons que le chiffrement est de plus en plus considéré comme étant l'un des contrôles de sécurité fondamentaux des organisations lors de leur migration vers le Cloud. Par le biais du chiffrement et d'une gestion des clés et politiques de sécurité associées, les organisations peuvent conserver la confiance des parties prenantes tout en adoptant l'offre Cloud.

Un accès sécurisé à SaaS

L'authentification multi-facteurs, que ce soit par le biais de tokens du type OTP (mot de passe à usage unique), de certificats, de tokens USB ou de cartes à puce, est devenue de plus en plus vitale dans les organisations. Ces dernières cherchent à sécuriser l'accès à leurs systèmes par des utilisateurs distants. Les entreprises migrent de plus en plus fréquemment des services stratégiques vers le Cloud et, de ce fait, les équipes de sécurité se doivent de mettre en place les mécanismes centralisés qui exploitent aussi bien les scénarios traditionnels d'accès à distance que les déploiements Cloud.

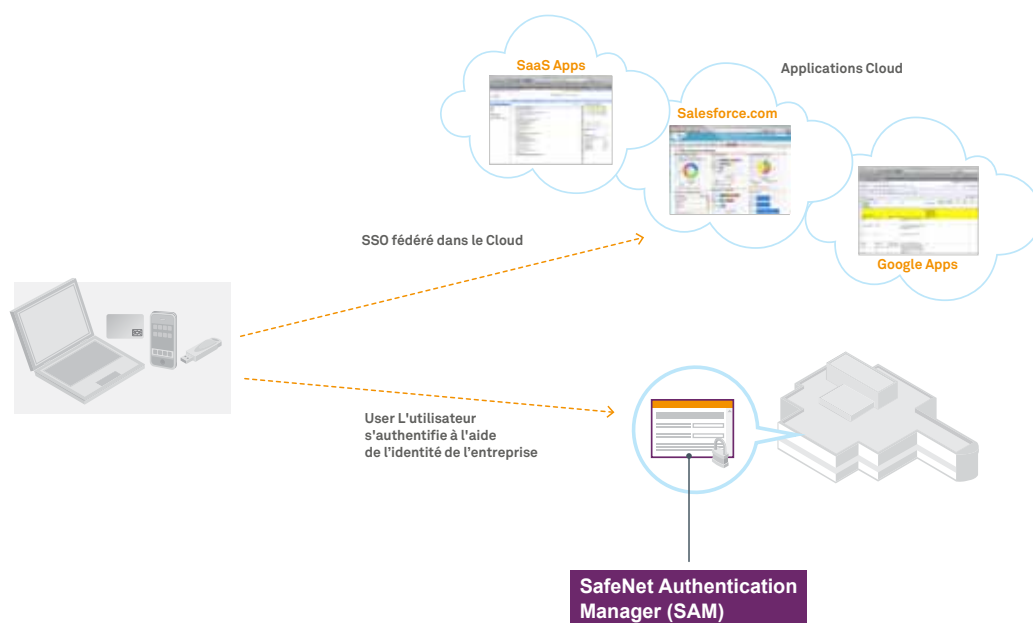
La solution

Avec le gestionnaire d'authentification de SafeNet (Safenet Authentication Manager), les clients peuvent tirer profit d'une infrastructure d'authentification unifiée, fonctionnant tant pour les services physiques (implantés dans leurs locaux) que pour les services basés sur le Cloud. Cela permet de disposer d'un moyen centralisé et complet de gestion de toutes les politiques d'accès. Lorsque des utilisateurs cherchent à accéder à l'un des services Cloud de l'entreprise (par exemple, un service SaaS comme Salesforce.com ou GoogleApps), ils doivent s'authentifier en utilisant leurs moyens existants d'authentification SafeNet (il peut s'agir de cartes à puce, de tokens USB ou de mots de passe OTP) depuis leur téléphone ou ordinateur portable.

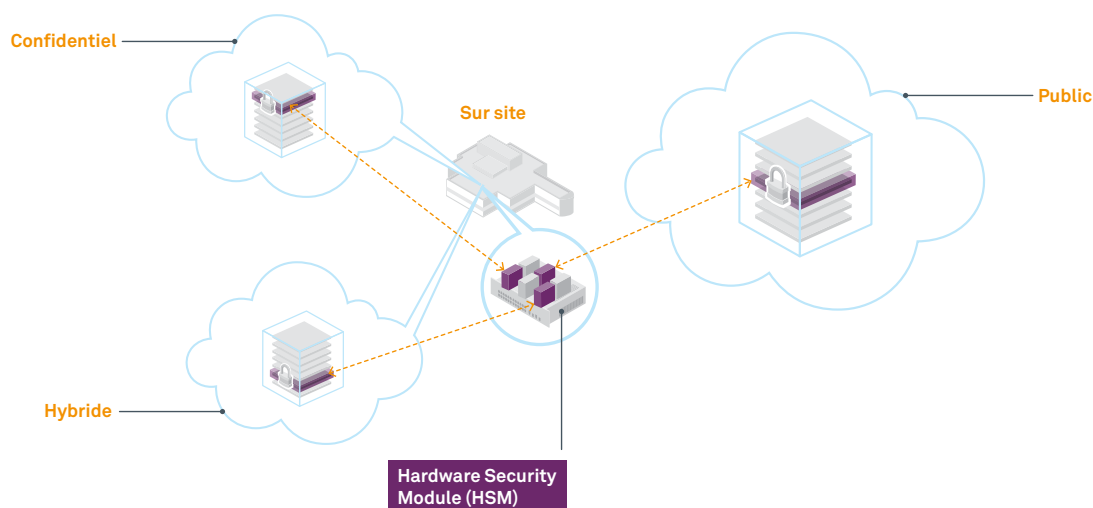
Les avantages

Les solutions complètes d'authentification de SafeNet permettent aux entreprises de maximiser plus facilement la sécurisation de l'authentification des applications SaaS. Les solutions SafeNet offrent une panoplie d'avantages sans égal aux entreprises qui passent au Cloud.

- **Une plate-forme complète.** Toutes les solutions SafeNet peuvent être gérées par le biais du gestionnaire d'authentification de SafeNet (Safenet Authentication Manager), qui est en fait un serveur central de gestion qui est chargé de fédérer les identités, de contrôler les accès et d'effectuer des authentifications fortes aux applications traditionnelles et aux applications SaaS.



- **Une flexibilité pour le déploiement sous une multitude de formats.** SafeNet propose le portefeuille d'authentification le plus complet (dont des tokens matériels, l'authentification logicielle, des solutions à mots de passe à usage unique OTP, pour ne citer que quelques exemples), ce qui fait que les entreprises ont des solutions adaptées à leurs besoins spécifiques.
- **Des fonctionnalités de reporting évoluées.** Les plates-formes d'authentification SafeNet offrent des fonctionnalités très larges de reporting qui simplifient le respect d'un très grand nombre de réglementations et politiques de sécurité.



Des identités et transactions sécurisées

De par sa nature virtualisée, le Cloud permet de se passer d'un grand nombre de points de contrôle basés sur le flux réel de travail et sur les périphériques qui avaient facilité la sécurisation des informations sensibles dans des déploiements internes traditionnels. Pour adopter les services Cloud, tout en maintenant les niveaux requis de confiance et de sécurité, les entreprises doivent adopter une approche de la sécurité centrée sur les données. Pour cela, il faut faire appel à des activités cryptographiques (dont le chiffrement des données et les signatures numériques) pour garantir le caractère confidentiel et l'intégrité des données informatiques et des processus. Simultanément, l'emploi de la cryptographie ne doit pas nuire à la performance et à la fiabilité des ressources du Cloud

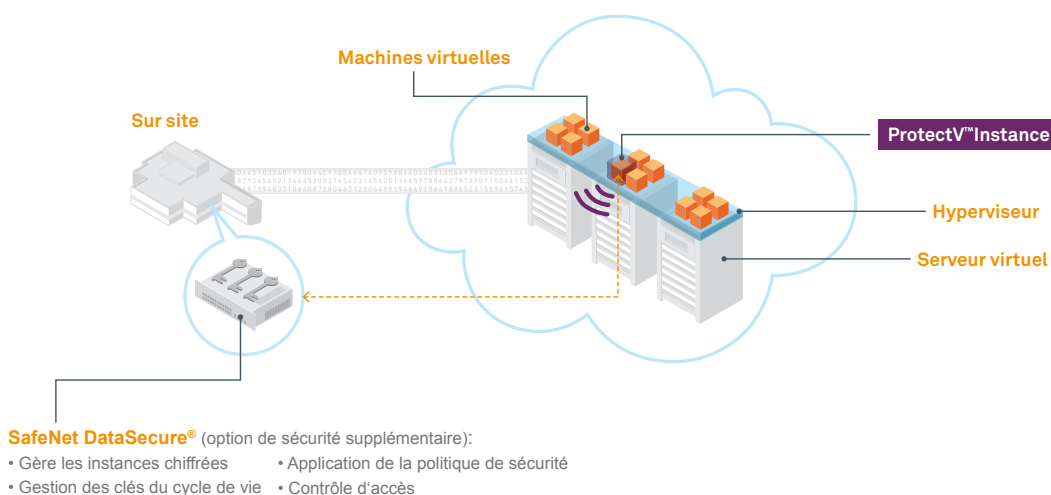
La solution

SafeNet offre les HSM (Hardware Security Modules) les plus sophistiqués et les plus sécurisés disponibles en réseau. Ils sont idéalement placés pour faire face aux demandes des infrastructures virtuelles et Cloud. Les HSM de SafeNet (dont SafeNet Luna SA) offrent une combinaison sans pareille de fonctionnalités (dont la gestion centralisée des clés et des politiques, un support robuste du chiffrement, une intégration flexible et bien d'autres) qui servent de base à la création d'une plate-forme Cloud sécurisée. Qui plus est, SafeNet est le seul prestataire qui offre des solutions HSM pour protéger les clés, permettant ainsi aux clés cryptographiques, qui sont essentielles pour garantir que vos applications et vos informations sensibles, de ne jamais sortir du cadre de vos périphériques (appliances). Enfin, SafeNet propose des HSM adaptés à FIPS et Common Criteria qui garantissent un stockage certifié des clés cryptographiques.

Les avantages

En employant des HSM de SafeNet dans leurs environnements Cloud, les entreprises sont en mesure d'en tirer un grand nombre d'avantages notables:

- **Optimisation de la sécurité.** SafeNet permet aux organisations de conserver un contrôle efficace par le biais de politiques de groupes, de contrôles efficaces d'accès par les utilisateurs et d'une gestion centralisée des clés et politiques de systèmes à distance. Equipées des fonctionnalités complètes et sophistiquées des HSM de SafeNet, les organisations peuvent cumuler de manière efficace les nombreux avantages des services Cloud tout en respectant tous les mandats pertinents en matière de réglementations et toutes les politiques associées de sécurité.
- **Réduction des coûts administratifs et des frais généraux.** Associant les avantages de sécurité des HSMs au modèle de fourniture du Cloud, les mises en œuvre de sécurité peuvent être nettement meilleur marché que les déploiements internes traditionnels en mettant, pour la première fois, des fonctionnalités de sécurité à la pointe de la technologie à la portée de toutes entreprises, y compris les PME.
- **Réalisation durable d'une flexibilité et d'une progression évolutive.** Chaque HSM de SafeNet peut supporter un maximum de 100 clients et 20 partitions, ce qui permet aux organisations de rentabiliser au mieux leurs investissements tout en bénéficiant d'un dispositif parfaitement évolutif et flexible permettant de faire face aux changements de leur volume d'activités et aux obligations techniques.



Des instances virtuelles sécurisées

Aujourd'hui, les entreprises migrent leurs serveurs des datacenters traditionnels vers des infrastructures virtualisées et partagées qui sont implantées dans des Clouds publics ou privés. Etant donné que ces serveurs virtuels hébergent souvent des applications et des banques de données qui contiennent des informations sensibles d'entreprises (dont les fichiers du personnel, les propriétés intellectuelles, les informations sur les clients et bien d'autres choses), la perte ou le vol de ces actifs virtuels peut s'avérer désastreux.

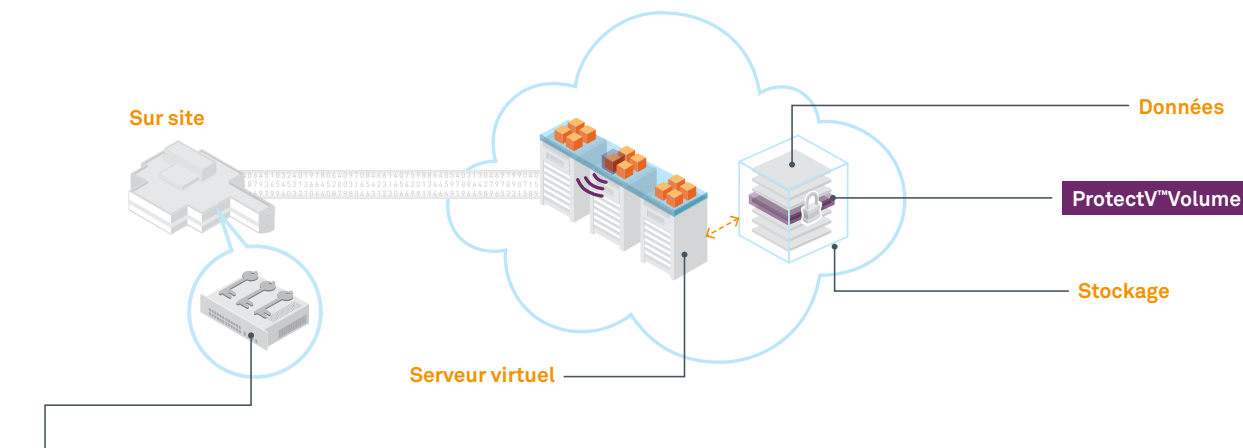
Pour respecter leurs obligations réglementaires ou leurs politiques internes de gestion du risque, les entreprises doivent relever une multitude de défis posés par les serveurs virtualisés et toutes les instances qu'ils contiennent (dont le contrôle de l'accès privilégié des administrateurs, la protection contre les copies potentielles illimitées, le contournement du problème dû à un manque de visibilité et d'auditabilité, et la réduction des risques auxquels sont exposées les données brutes). Pour relever ces challenges et protéger les informations sensibles que détiennent les serveurs virtuels, les organisations doivent aller au-delà des contrôles simples d'accès par les utilisateurs et doivent en fait activement sécuriser les serveurs virtuels.

La solution

Pour minimiser les risques que peuvent faire courir les serveurs virtuels aux données sensibles, SafeNet propose ProtectV Instance qui permet aux organisations de chiffrer et sécuriser tout le contenu des serveurs virtuels, en protégeant ainsi ces biens contre le vol ou le risque d'exposition. Grâce à ProtectV Instance, les données que contient le lecteur sont sécurisées, même hors ligne et pendant l'activation de l'instance. ProtectV Instance assure la séparation essentielle des tâches pour le contrôle de serveurs virtuels et ajoute la visibilité vitale nécessaire pour assurer un audit des serveurs basés sur le Cloud.

Les avantages

En tirant profit du chiffrement sur tout le disque des serveurs virtuels dans le Cloud, les entreprises sont en mesure de rester propriétaires de leurs données sensibles et d'en assurer le contrôle et, de ce fait, de se protéger contre les dégâts que pourraient provoquer un vol ou une manipulation sans autorisation. Même en cas de réplication d'une image virtuelle d'un ordinateur portable perdu, les équipes chargées de la sécurité conservent la certitude que leurs données sensibles ne seront pas exposées à un accès non autorisé. Avec ProtectV Instance, les organisations peuvent maximiser les avantages qu'offrent leurs déploiements dans des Clouds privés et publics, y compris une infrastructure de service (IaaS), sans compromettre la sécurité.



SafeNet DataSecure® (option de sécurité supplémentaire):

- Gère les instances chiffrées
- Application de la politique de sécurité
- Gestion des clés du cycle de vie
- Contrôle d'accès

Un stockage sécurisé basé sur le Cloud

Pour de nombreuses organisations, la perspective de profiter de services flexibles en ne payant que les services utilisés pour héberger des volumes croissants de fichiers et d'actifs numériques représente une réelle opportunité. Néanmoins, pour de nombreuses organisations, en particulier celles qui doivent respecter des obligations réglementaires spécifiques, les risques de sécurité posés par la conservation d'informations dans des serveurs de stockage mutualisés, font que le Cloud est tout de suite éliminé des solutions envisageables.

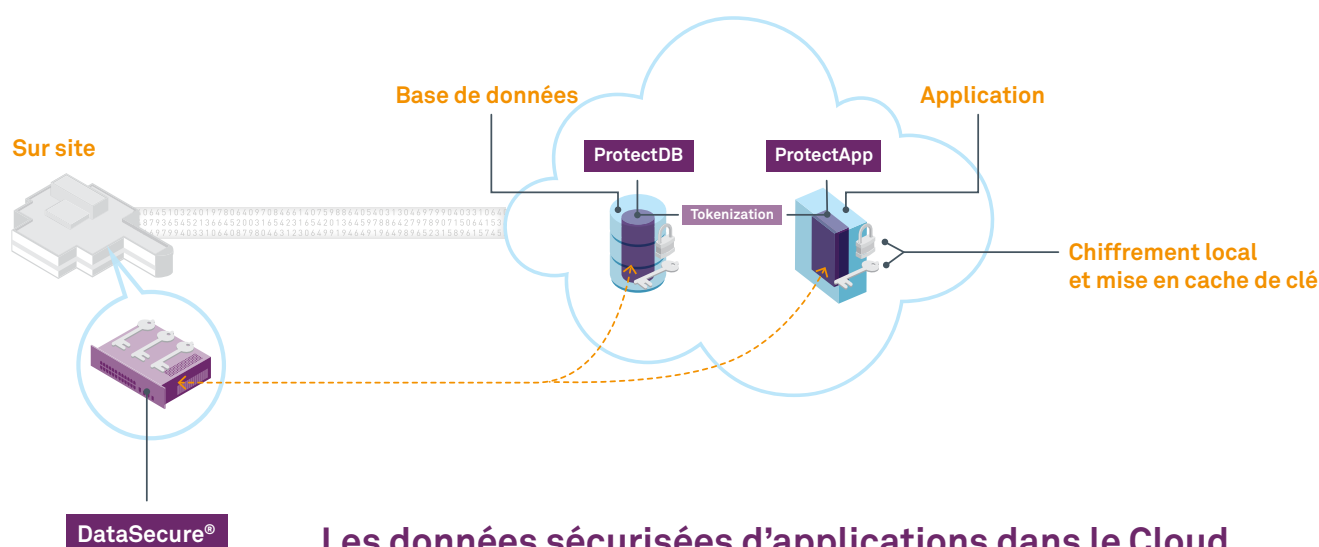
La solution

Grâce à ProtectV Volume, les équipes chargées de la sécurité peuvent chiffrer des volumes complets de stockage dans le cadre de déploiements Cloud, entraînant ainsi l'isolement et la sécurisation des données Cloud, et ce même dans des services de stockage Cloud partagés et mutualisés. Du fait de son intégration discrète, ProtectV Volume peut se déployer dans un large éventail d'environnements de stockage basé sur le Cloud, quel que soit le fournisseur ou la technologie sous-jacente de stockage.

Les avantages

Avec ProtectV Volume de SafeNet, les entreprises peuvent optimiser un grand nombre des avantages offerts par les services Cloud, tout en maintenant des contrôles de sécurité efficaces. Avec ProtectV Volume de SafeNet, les organisations peuvent profiter du Cloud et l'intégrer à des applications qui jusque là se situaient en dehors des limites du point de vue de la sécurité. Avec SafeNet, les entreprises peuvent engranger un grand nombre d'avantages.

- **Doper la productivité de l'utilisateur.** Grâce à une mise en œuvre transparente et discrète, les solutions SafeNet permettent aux utilisateurs autorisés de profiter d'un accès plus homogène et plus fiable d'une manière à la fois discrète et transparente, qui favorise la productivité.
- **Réduction des coûts.** Grâce à une mise en application complète et cohérente des règles de sécurité dans le Cloud, les solutions SafeNet permettent aux organisations de migrer un plus grand nombre de services dans le Cloud et, par conséquent, de bénéficier des réductions de coûts élevées que ces modèles offrent. En outre, en centralisant et simplifiant l'administration, la gestion et la mise en application de la sécurité, les solutions SafeNet permettent de réduire sensiblement les coûts.
- **Augmentation de l'agilité de l'entreprise.** Les éléments concrets que propose le Cloud permettent, de manière intrinsèque, aux organisations de s'adapter et de s'engager bien plus vite et en bénéficiant d'un rapport qualité/prix bien meilleur que dans des infrastructures hébergées en interne. Grâce au support accordé aux environnements Cloud dynamiques, les solutions SafeNet sont en mesure d'offrir aux organisations des capacités sans pareil pour profiter au mieux de la flexibilité du Cloud et s'adapter ainsi plus rapidement à l'évolution de leurs besoins.



Les données sécurisées d'applications dans le Cloud

Pour toute entreprise, il est vital de préserver la confiance de ses clients. Bien que la migration d'applications vers le SaaS et le Paas permettent à une organisation de réduire fortement ses coûts, et d'offrir un accès omniprésent aux utilisateurs, ce changement signifie que les données vitales des clients vont résider dans un environnement que cette organisation ne possède ou ne contrôle pas. Si cette application n'offrait pas de protection active des données y entrant, les risques potentiels associés à une telle perte de contrôle et de confiance seraient potentiellement dramatiques.

Pour satisfaire les avantages économiques et les obligations en matière de sécurité des applications basées sur le Cloud, les organisations doivent respecter plusieurs dispositions centrales:

- **Une intégration transparente des applications.** Les organisations doivent être en mesure de chiffrer les données se trouvant dans leur propre environnement de développement d'applications, en faisant appel à une simple intégration ne les obligeant pas à devenir des experts en cryptographie.
- **Une gestion et un contrôle centralisés.** Le contrôle des données doit être centralisé afin de minimiser les coûts opérationnels et d'offrir les fonctionnalités requises pour assurer les tâches administratives d'audits et de séparation.
- **Un déploiement flexible et agile.** Etant donné qu'elles vont faire appel à plusieurs prestataires offrant des services Cloud et changer de prestataires de temps en temps, les organisations ont besoin d'outils de contrôle flexibles pour la protection des données lors des transferts vers d'autres fournisseurs.

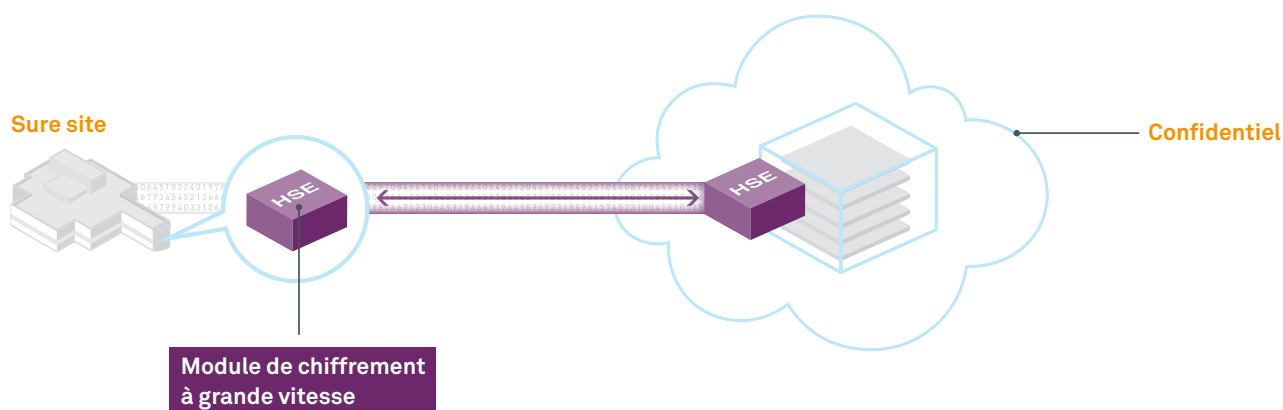
La solution

Pour préserver la sécurité et la continuité commerciale, lors du passage au Cloud, les entreprises peuvent déployer DataSecure en local et configurer et activer ProtectApp de manière à sécuriser les applications virtualisées qui manipulent diverses données sensibles dont, entre autres, les cartes de crédit et les informations personnellement identifiables. ProtectApp est ainsi proposé pour un large éventail de plate-formes de déploiement afin de permettre une intégration transparente alors que le contrôle centralisé via DataSecure offre la flexibilité requise pour travailler avec plusieurs prestataires de services Cloud. La plate-forme DataSecure, qui s'exploite en local, vient s'ancrer pour devenir la base de la confiance concernant la mise en œuvre des politiques et la gestion du cycle de vie des clés.

Dans un environnement Cloud, ProtectApp assure le chiffrement et la saisie des clés, en local, pour optimiser les performances. Comme les données sont protégées au fur et à mesure de leur création et stockées dans les bases de données du Cloud et que les clés sont conservées avec le serveur d'applications, l'entreprise a la certitude que ses données sensibles vont rester sécurisées et être en conformité avec les mandats les concernant.

Les avantages

Grâce à SafeNet, les organisations peuvent se servir du SaaS et du PaaS pour leurs applications, tout en protégeant les données de leurs clients. En outre, la flexibilité de cette solution permet de déployer ces protections avec un minimum de frais et un maximum d'agilité, qui permet de travailler avec les nombreux fournisseurs de solutions dans le Cloud.



Les communications sécurisées dans le Cloud

Qu'une organisation décide de se lancer, doucement ou fortement, dans des services basés sur le Cloud, la réalité est la suivante : chaque entreprise, ou presque, aura mis en place, à un moment ou un autre, un mélange hybride de services (en local et / ou dans un Cloud privé ou public). De ce fait, il faut souvent acheminer les actifs sensibles d'une organisation sur un réseau élargi (WAN) sous la forme de données et de leurs traitements, répartis entre les déploiements distribués sur le plan géographique. Pour bâtir une infrastructure de confiance qui associe plusieurs sites hybrides, les entreprises doivent faire appel au chiffrement pour sécuriser cet acheminement des données sur leurs réseaux WAN, tout en garantissant l'établissement de communications rapides et à faible latence entre ces différents sites.

La solution

Aujourd'hui, SafeNet propose des solutions sophistiquées de chiffrement de niveau 2 qui permettent aux organisations de sécuriser leurs communications WAN, tout en évitant les défis au niveau des performances et les obstacles que présentent les approches traditionnelles de chiffrement IPsec. Le logiciel de chiffrement Ethernet Encryptors de SafeNet offre une grande efficacité administrative, des performances optimisées et une exploitation sur une large bande passante qui font que ce logiciel est la solution idéale dans l'environnement Cloud privé d'une entreprise.

Les avantages

Grâce aux logiciels de chiffrement Ethernet Encryptors de SafeNet, les organisations sont en mesure de maintenir des communications de confiance dans tous leurs sites internes et basés sur le Cloud, tout en profitant d'un grand nombre d'avantages.

- **Coup de pouce à la productivité de l'utilisateur.** Grâce à ses excellentes performances et sa grande fiabilité, SafeNet permet aux utilisateurs autorisés de transférer rapidement et en toute sécurité des communications, des supports et d'autres données vers le Cloud – ce qui optimise la productivité.
- **Réduction des coûts.** En éliminant les frais généraux coûteux que représentent les circuits de transport et en garantissant une cadence optimale, SafeNet permet de réduire immédiatement les coûts au niveau du Cloud et dans toute l'entreprise. En outre, au fur et à mesure de l'évolution des modèles basés sur le Cloud, les entreprises peuvent facilement ajouter de nouvelles fonctionnalités à leur environnement Cloud opérationnel. En centralisant et simplifiant l'administration, la gestion et la mise en application de la sécurité, SafeNet permet de réduire sensiblement les coûts.
- **Augmentation de l'agilité de l'entreprise.** Les éléments que propose le Cloud permettent, de manière intrinsèque, aux organisations de s'adapter et de s'engager bien plus vite tout en bénéficiant d'un rapport qualité/prix bien meilleur que dans des infrastructures réseaux hébergées en local. Grâce au soutien accordé aux environnements Cloud dynamiques, SafeNet est en mesure d'offrir aux organisations des capacités sans pareil pour profiter au mieux de la flexibilité du Cloud et s'adapter ainsi plus rapidement à l'évolution de leurs besoins.

Le Trusted Cloud Fabric de SafeNet

SafeNet propose la Structure Cloud de Confiance la plus complète pour les environnements virtualisés. Son objectif est de créer et de maintenir la confiance des organisations, tout au long du cycle de vie des données de ces entreprises. Le Trusted Cloud Fabric™ de SafeNet représente un écosystème complet qui relie une protection persistante, un chiffrement flexible, une identité reposant sur des ancrés de sécurité et des communications sécurisées. Grâce à toutes ces fonctionnalités, les clients SafeNet prennent pleinement confiance. Ils conservent la propriété et la maîtrise totale des activités d'isolement, de protection et de partage de leurs données, même dans des environnements Cloud mutualisés. Prolongement du système de Protection du cycle de vie de l'information de SafeNet, le Trusted Cloud Fabric™ permet aux clients d'intégrer en douceur le modèle Cloud souhaité à leurs stratégies de sécurisation à court et long terme.

A propos de SafeNet, Inc.

Fondé en 1983, SafeNet est l'un des leaders mondiaux de la sécurisation des informations. SafeNet protège les biens de ses clients qui ont la plus grande valeur: entre autres, les identités, transactions, communications, données et licences logicielles tout au long du cycle de vie de ces informations. Plus de 25 000 clients, des grands comptes aux administrations, répartis dans plus de 100 pays du monde entier, font confiance à SafeNet pour sécuriser leurs informations.

Contactez-nous: Pour connaître les adresses de nos services et pour nous contacter, visitez www.safenet-inc.com
Vous pouvez nous suivre à: www.safenet-inc.com/connected

©2011 SafeNet, Inc. Tous droits réservés. SafeNet et le logo SafeNet sont de marques commerciales déposées de SafeNet. Tous les autres noms de produits sont des marques commerciales de leurs propriétaires respectifs. Security_Practioners_Guide_TCF_WP_(FR)_A4_26.4.11

