THALES
Building a future we can all trust

artilcle

Simplifier la souveraineté numérique dans un environnement de multi-cloud

Maintenir un contrôle rigoureux des données sensibles est essentiel à la réussite des entreprises numériques, mais comment gérer cette complexité ?

La souveraineté est traditionnellement définie comme la capacité d'un État à se gouverner lui-même et à gouverner ses sujets, et elle est à l'ordre du jour depuis le début de la civilisation. Mais ce n'est que récemment que la souveraineté numérique, soit la capacité de contrôler ses propres actifs numériques et de prendre des décisions à leur sujet, a émergé pour devenir un sujet à part entière.

« De manière générale, la souveraineté numérique signifie avoir le contrôle de son destin numérique », explique Tim Phipps, directeur des alliances cloud au sein du groupe technologique français Thales. « Un niveau plus bas, cela signifie que vous contrôlez totalement les logiciels, le matériel et les données dont dépend votre entreprise. »

Maîtriser son destin numérique ne semblait peut-être pas important lorsque l'informatique se limitait à gérer un système de paie échelonné. Aujourd'hui, lorsque les entreprises prospèrent et périssent selon leur utilisation de la technologie qui couvre de multiples dispositifs, systèmes, applications, charges de travail et lieux d'hébergement, la question est beaucoup plus centrale.

C'est plus particulièrement d'un problème pour les fournisseurs de services cloud qui n'ont plus l'habitude de conserver leurs données au même endroit. Plus de 90 % des organisations ont désormais une stratégie de cloud multiple, selon un récent rapport Thales sur les menaces informatiques. Le rapport a également révélé que des entreprises mélangeaient ces environnements de cloud multiples avec des opérations sur site et des centres de données co-localisés, brouillant encore davantage les pistes.

Cela présente un certain nombre de défis, notamment les coûts liés à la gestion de plusieurs magasins de clés de chiffrement et de processus de gestion à mesure que davantage de données sont transférées vers le cloud, par exemple. Cela implique que les organisations doivent généralement faire appel à différentes équipes pour gérer différentes solutions de gestion des clés, ce qui représente un défi en matière de recrutement en soi. Ces organisations courent également le risque d'étendre la surface d'attaque des pirates informatiques en mettant en place une série de solutions de sécurité des données disparates, chacune d'entre elles appliquant des politiques et des processus de sécurité différents.

À l'instar d'Internet, la souveraineté numérique semble donc assez simple, mais il s'agit d'un concept plus complexe qu'il n'y paraît, impliquant différentes composantes. Pour aider les organisations à comprendre et à relever ces défis, Thales décompose la souveraineté en trois éléments : les données, les opérations et les logiciels.

Souveraineté des données

Les données sont l'élément auquel beaucoup pensent en premier lorsqu'ils entendent le terme de souveraineté numérique. Il s'agit de la capacité d'un État à protéger ses propres données et celles de ses citoyens contre les intrusions d'autres États. Cette question a été au cœur de la gouvernance d'Internet au cours des deux dernières décennies.

« Ce qui inquiétait les nations, surtout en Europe, c'est que beaucoup de ces fournisseurs de cloud (ou hyperscalers) sont tous américains », souligne M. Phipps. « Les lois américaines sur l'espionnage suscitaient toutes sortes d'inquiétudes. »

Le Patriot Act comprenait une formulation qui accordait aux autorités américaines un accès possible aux dossiers commerciaux des fournisseurs de services cloud, ce qui, Microsoft l'a admis plus tard, mettait en péril la confidentialité des dossiers des clients non nationaux si le gouvernement américain les demandait. Le CLOUD Act, introduit en 2018, a par la suite solidifié la capacité des enquêteurs gouvernementaux à obtenir des fichiers auprès de fournisseurs traitant des données sur le sol étranger.

Dans le même temps, les défenseurs de la protection de la confidentialité se sont opposés à l'échange de données entre les fournisseurs américains et européens. La disposition relative à la sphère de sécurité (Safe Harbour) permettait aux fournisseurs américains de transférer aux États-Unis des données provenant de partenaires de l'UE s'ils s'engageaient à respecter plusieurs principes en matière de protection de la confidentialité. Max Schrems, avocat et défenseur de la protection de la confidentialité, a contesté cette disposition en 2015, ce qui a conduit à son annulation et à son remplacement par l'accord sur le bouclier de protection des données UE-États Unis (EU-US Privacy Shield). M. Schrems a également contesté cette décision, qui a été déclarée invalide en 2020.

Aujourd'hui, l'Union européenne et les États-Unis s'attaquent une troisième fois au problème avec le cadre transatlantique de protection des données. Un projet de décision d'adéquation, qui tente de remplacer la « décision relative au bouclier de protection des données », invalidée par la suite par l'arrêt Schrems II, a été très récemment publié par l'UE.

D'après les premières réactions de Max Schrems, le projet de décision est presque entièrement basé sur le décret connu qui a été rejeté précédemment. Il est probable que l'équipe de Max Schrems contestera cette décision devant les tribunaux européens. Par conséquent, les entreprises des deux côtés de l'Atlantique restent dans le flou quant à la suite des événements, ce qui peut faire stagner les projets de transformation numérique.

M. Phipps recommande aux organisations de mettre en place des contrôles appropriés pour protéger leurs actifs numériques, afin qu'elles puissent détenir leur propre souveraineté en matière de données et accélérer leur passage au cloud, indépendamment des changements géopolitiques.

Cependant, cela peut représenter un défi considérable dans un environnement de cloud multiple et hybride. Près d'une personne sur cinq ayant répondu à l'enquête de Thales a déclaré ne pas savoir où sont stockées toutes ses données. Environ la moitié a déclaré que la gestion de leurs données sensibles dans des environnements de cloud multiple est plus difficile que sur site. Cette situation peut avoir de graves conséquences. L'enquête de Thales a également révélé que 35 % des personnes interrogées ont subi des fuites de données ou des échecs de vérifiabilité de données et d'applications basées sur le cloud au cours de l'année écoulée.

Souveraineté opérationnelle et logicielle

Selon M. Phipps, la deuxième catégorie de souveraineté numérique est opérationnelle. « Il s'agit du cas où vous avez vos données dans le cloud et que vous vous inquiétez d'une menace interne ou d'acteurs malveillants », explique-t-il. « Cela peut être un ingénieur du cloud, mais cela peut aussi être votre propre personnel. » Un employé malhonnête cherchant à obtenir un gain financier personnel pourrait voler vos données, tout comme un travailleur mécontent de votre entreprise, éventuellement à la demande d'un tiers.

La menace pour la souveraineté opérationnelle peut également se présenter sous la forme d'un programme malveillant, d'une application corrompue ou d'un ransomware qui a récupéré les identifiants de connexion d'un utilisateur privilégié afin d'obtenir un accès élargi à des données ou des systèmes sensibles.

Enfin, Thales cite la souveraineté logicielle comme un problème pour les entreprises. « Il s'agit de la possibilité d'exécuter vos charges de travail où vous le souhaitez », déclare M. Phipps.

Les entreprises veulent de plus en plus avoir le choix lorsqu'elles passent au cloud. Elles pourraient vouloir exécuter la plupart de leurs charges de travail avec un fournisseur de cloud spécifique afin d'obtenir de meilleures conditions commerciales, explique-t-il. Mais les régulateurs craignent que, s'il n'y a pas de possibilité de procéder à une sortie contrôlée et rapide de la crise, ces entreprises mettent tous leurs œufs dans le même panier. Les organisations sont encouragées à s'assurer que leurs charges de travail critiques sont sécurisées et transférables, ce qui contribue à garantir la résilience opérationnelle et la continuité des activités en cas de problème.

Par exemple, l'Autorité de régulation prudentielle de la Banque d'Angleterre, qui a succédé à l'Autorité des services financiers, s'est inquiétée de la dépendance des banques à l'égard du cloud computing à partir d'un fournisseur unique. Elle recommande aux institutions de services financiers d'adopter des architectures de cloud multiple afin de répartir les risques et d'éviter le verrouillage des fournisseurs, tandis que la loi sur la résilience opérationnelle numérique aussi appelée DORA (Digital Operational Resilience Act) dans l'UE préconise une approche similaire.

Par conséquent, les banques sont contraintes de partager leurs charges de travail et d'avoir des fournisseurs cloud de secours vers lesquels elles peuvent basculer en cas de panne ou de rupture de la relation.

Protection de la souveraineté numérique en pratique

Thales s'est fait un devoir de répondre à ces diverses exigences en matière de souveraineté. Elle utilise un processus en quatre étapes pour amener ses clients sur un terrain positif où ils se sentent totalement maîtres de leurs données, de leurs opérations et de leurs logiciels.

L'entreprise commence par un processus de découverte. Après tout, on ne peut pas contrôler ce que l'on ne connaît pas. L'entreprise cherche donc à répondre à des questions telles que : où se trouvent nos données et quelles sont-elles ? Dans quelle mesure sont-elles sensibles ?

Selon M. Phipps, de nombreuses organisations ne connaissent pas ces informations de base. Les entreprises génèrent en permanence de nouvelles données et il ne s'agit plus simplement de classer les registres de la base de données dans des champs connus. « De plus en plus, une grande partie des données sensibles générées sont non structurées et apparaissent dans des endroits aléatoires », affirme-t-il. L'adoption grandissante du cloud et les politiques modernes de travail à distance ont contribué à ce que 2,5 trillions d'octets de nouvelles données soient générés chaque jour dans les e-mails, les présentations et les feuilles de calcul, selon certaines estimations. Sans aide extérieure, il est beaucoup plus difficile de localiser les informations sensibles contenues dans ces vastes volumes.

À cette fin, Thales a développé la solution Data Discovery and Classification (DDC), qui recherche des types de données spécifiques en fonction des modèles de conformité auxquels l'organisation s'intéresse. DDC utilise des algorithmes d'apprentissage automatique, ainsi qu'une bibliothèque de référence de modèles prédéfinis de

confidentialité des données et de réglementation, tels que le RGPD, la CCPA, la LGPD, PCI DSS et HIPAA, pour trouver les données sensibles d'intérêt et appliquer une note de risque basée sur les politiques et la conformité du client. DDC peut alors recommander une remédiation manuelle ou l'appliquer automatiquement, ce qui permet de gagner du temps et de minimiser la surface d'attaque.

Protection par chiffrement multicouche

À quoi ressemble cette remédiation ? C'est là qu'intervient la deuxième étape de la méthodologie de Thales, à savoir la protection. Elle se concentre principalement sur le chiffrement multicouche, qu'elle divise en trois types : les données au repos, en transit et en cours d'utilisation.

Comme le souligne M. Phipps, tous les grands fournisseurs de cloud chiffrent par défaut les données au repos. Mais il y a un bémol : nombre d'entre eux ne les chiffrent qu'au niveau du disque. Cela peut empêcher quelqu'un de récupérer les données dans le cas peu probable où il volerait un disque physique dans le centre de données du cloud, mais que se passerait-il s'il détournait le compte d'une personne à distance ? Peu de fournisseurs de cloud, si ce n'est aucun, chiffrent automatiquement les données au-dessus du niveau du disque, par exemple au niveau du fichier, de la base de données ou de l'application, ce qui peut contribuer à atténuer cette menace.

Thales propose des solutions pour chiffrer les données à plusieurs niveaux, y compris les données structurées et non structurées, afin de mettre en place une défense en profondeur. Le chiffrement transparent au niveau des fichiers protège l'ensemble de la base de données pour un surcoût de performance d'environ 2 %, explique M. Phipps. Les clients peuvent appliquer des niveaux de chiffrement plus élevés à des champs spécifiques de la base de données s'ils le souhaitent.

Bien que cela impose un surcoût en matière de performances, cela permet également de renforcer les niveaux de protection là où cela est nécessaire. La sécurité, la conformité et les performances font souvent l'objet de compromis. L'essentiel est d'adopter une approche fondée sur le risque pour s'assurer que la protection appliquée de manière appropriée est basée sur les résultats souhaités par l'entreprise.

En ce qui concerne le chiffrement en transit, TLS est la norme de facto. Toutefois, M. Phipps fait valoir que cela peut souvent s'avérer problématique compte tenu des importants volumes de données que certains fournisseurs traitent dans le cloud. Au lieu de cela, Thales propose un chiffrement à haut débit dans ses produits de chiffreurs réseau, qui, selon M. Phipps, sont plus rapides que TLS et offrent un degré de protection plus élevé.

Thales met également l'accent sur le chiffrement des données en cours d'utilisation, qui permet de lutter contre le sabotage ou l'espionnage pendant le traitement sur le cloud. « Nous avons discuté avec des fournisseurs d'infrastructures critiques, tels que des fournisseurs d'énergie, et ils s'inquiètent de l'exécution de charges de travail sensibles dans le cloud pour des applications critiques en ce qui concerne la sécurité », explique M. Phipps. « Si quelqu'un injecte un programme malveillant dans une puce qui traite des données, il peut effectivement procéder à un déni d'accès et mettre tout le système hors service. »

Pour lutter contre ce phénomène, les fournisseurs du cloud travaillent sur diverses initiatives d'informatique confidentielle. Dans ces services, une partie de la puce devient une enclave sécurisée sous le contrôle du client plutôt que du fournisseur de services du cloud. Microsoft Azure, Google Cloud et AWS proposent tous des offres dans ce domaine.

Maintenir la souveraineté des données dans le cloud

Le troisième pilier du service de souveraineté numérique de Thales concerne le contrôle. Le fait de laisser ces clés de chiffrement dans le cloud les place théoriquement sous le contrôle du fournisseur de services du cloud, ce qui constitue une menace évidente pour la souveraineté du client. Cela rend le client vulnérable aux comportements malveillants ou aux erreurs d'un tiers, comme les propres ingénieurs d'assistance du fournisseur de services du cloud. Les données sont également menacées en cas d'assignation à comparaître d'un État étranger.

La solution à cette menace réside dans la séparation des tâches. La création et le stockage des clés de chiffrement en dehors du cloud, en les séparant de l'endroit où les données sensibles sont stockées, donnent au client un contrôle ultime sur les données. En cas de menace pour les données, le client peut conserver les clés. Comme le fournisseur de services du cloud ne peut pas accéder unilatéralement à ces clés, il ne peut pas être contraint de remettre les données à un tiers.

Certains fournisseurs du cloud ont mis en place des services permettant aux clients de stocker leurs propres clés pour les charges de travail basées sur le cloud, créant ainsi une séparation claire des tâches entre le fournisseur de services du cloud et le client. La gestion externe des clés (EKM) de Google Cloud en est un bon exemple.

Thales a collaboré avec Google Cloud pour aider ses clients à gérer le contrôle de leurs données, de leurs opérations et de leurs logiciels tout en bénéficiant des avantages du cloud computing. En décembre 2020, elles ont travaillé à l'intégration du service CipherTrust Key Broker de Thales avec l'EKM de Google Cloud. Cela permet aux clients de générer leurs clés de chiffrement pour le service cloud de Google tout en conservant les clés en dehors de l'environnement de Google Cloud.

Depuis, les deux entreprises ont étendu leur partenariat à d'autres services. En juin 2021, CipherTrust Manager et le produit SafeNet Trusted Access de Thales ont été intégrés pour prendre en charge le chiffrement côté client du service Workspace de Google, par exemple. Les organisations peuvent ainsi chiffrer les données de Google Drive à l'aide de leurs propres clés.

L'année dernière, elles ont également collaboré à la mise en place d'une plateforme basée sur le cloud qui répond au label Trusted Cloud du gouvernement français. Cela oblige les fournisseurs de services du cloud à héberger leurs serveurs en France et à n'autoriser que les fournisseurs européens à exploiter ces serveurs en utilisant les citoyens européens tout en limitant les transferts de données vers d'autres pays. En outre, cela nécessite de définir une série d'exigences juridiques, physiques, opérationnelles et techniques.

En attendant, la co-entreprise détenue majoritairement par Thales avec Google Cloud, S3NS, permet déjà aux clients de Google Cloud en France de restreindre l'accès aux sites de l'UE, à l'aide de ses propres services de gestion des clés. S3NS gère les clés de haut niveau, les identités et les racines de confiance, ainsi que la vérification des mises à jour de Google Cloud et l'examen du code source. S3NS développe également un service conforme au Trusted Cloud, dont la sortie est prévue pour 2024.

L'unification des opérations et de la gestion des clés dans le cloud, tout en gardant les clés sous le contrôle du client, résout l'un des plus gros problèmes de la sécurité dans le cloud : la complexité de la gestion des clés. L'enquête de Thales a révélé que 57 % des entreprises utilisent au moins cinq solutions distinctes de gestion des clés, ce qui accroît la complexité et le coût de la gestion du chiffrement des données. Le regroupement et la simplification de cette gestion des clés deviendront de plus en plus critiques à mesure que les entreprises gèrent des données sensibles dans un environnement de plus en plus distribué.

Contrôler la souveraineté numérique dans le temps

Alors que les entreprises continuent d'étendre leurs numérisations dans des environnements de cloud multiples et hybrides complexes, elles ont besoin d'un moyen de garder une certaine visibilité. C'est là qu'intervient la dernière partie du processus de souveraineté numérique de Thales : le suivi. La plateforme CipherTrust de l'entreprise, actuellement disponible en tant que produit sur site mais bientôt lancée en tant que service, offre une vue unique de la souveraineté numérique sur l'ensemble de leurs outils et processus dans des environnements de cloud multiples et cloud hybrides. Le système permet d'accéder à une gamme de produits tiers en plus de DDC de Thales.

Les principes et les pratiques en matière de souveraineté numérique ne feront que se complexifier au fil du temps, estime M. Phipps. C'est pourquoi il insiste sur les avantages de l'intégration de la protection de la confidentialité dès la conception dans les architectures de cloud hybrides et multiples. Phipps insiste également sur la nécessité d'établir des relations humaines fondées sur la confiance et l'empathie, afin de maximiser l'expérience du client.

« La technologie seule, sans les bonnes relations avec les conseillers et les fournisseurs, ne permettra probablement pas au client de mieux comprendre la marche à suivre », conclut-il. C'est là un casse-tête difficile à résoudre dont seules une expertise externe et une approche collaborative peuvent venir à bout.

La souveraineté est traditionnellement définie comme la capacité d'un État à se gouverner lui-même et à gouverner ses sujets, et elle est à l'ordre du jour depuis le début de la civilisation. Mais ce n'est que récemment que la souveraineté numérique, soit la capacité de contrôler ses propres actifs numériques et de prendre des décisions à leur sujet, a émergé pour devenir un sujet à part entière.

« De manière générale, la souveraineté numérique signifie avoir le contrôle de son destin numérique », explique Tim Phipps, directeur des alliances cloud au sein du groupe technologique français Thales. « Un niveau plus bas, cela signifie que vous contrôlez totalement les logiciels, le matériel et les données dont dépend votre entreprise. »

Maîtriser son destin numérique ne semblait peut-être pas important lorsque l'informatique se limitait à gérer un système de paie échelonné. Aujourd'hui, lorsque les entreprises prospèrent et périssent selon leur utilisation de la technologie qui couvre de multiples dispositifs, systèmes, applications, charges de travail et lieux d'hébergement, la question est beaucoup plus centrale.

C'est plus particulièrement d'un problème pour les fournisseurs de services cloud qui n'ont plus l'habitude de conserver leurs données au même endroit. Plus de 90 % des organisations ont désormais une stratégie de cloud multiple, selon un récent rapport Thales sur les menaces informatiques. Le rapport a également révélé que des entreprises mélangeaient ces environnements de cloud multiples avec des opérations sur site et des centres de données co-localisés, brouillant encore davantage les pistes.

Cela présente un certain nombre de défis, notamment les coûts liés à la gestion de plusieurs magasins de clés de chiffrement et de processus de gestion à mesure que davantage de données sont transférées vers le cloud, par exemple. Cela implique que les organisations doivent généralement faire appel à différentes équipes pour gérer différentes solutions de gestion des clés, ce qui représente un défi en matière de recrutement en soi. Ces organisations courent également le risque d'étendre la surface d'attaque des pirates informatiques en mettant en place une série de solutions de sécurité des données disparates, chacune d'entre elles appliquant des politiques et des processus de sécurité différents.

À l'instar d'Internet, la souveraineté numérique semble donc assez simple, mais il s'agit d'un concept plus complexe qu'il n'y paraît, impliquant différentes composantes. Pour aider les organisations à comprendre et à relever ces défis, Thales décompose la souveraineté en trois éléments : les données, les opérations et les logiciels.

Souveraineté des données

Les données sont l'élément auquel beaucoup pensent en premier lorsqu'ils entendent le terme de souveraineté numérique. Il s'agit de la capacité d'un État à protéger ses propres données et celles de ses citoyens contre les intrusions d'autres États. Cette question a été au cœur de la gouvernance d'Internet au cours des deux dernières décennies.

« Ce qui inquiétait les nations, surtout en Europe, c'est que beaucoup de ces fournisseurs de cloud (ou hyperscalers) sont tous américains », souligne M. Phipps. « Les lois américaines sur l'espionnage suscitaient toutes sortes d'inquiétudes. »

Le Patriot Act comprenait une formulation qui accordait aux autorités américaines un accès possible aux dossiers commerciaux des fournisseurs de services cloud, ce qui, Microsoft l'a admis plus tard, mettait en péril la confidentialité des dossiers des clients non nationaux si le gouvernement américain les demandait. Le CLOUD Act, introduit en 2018, a par la suite solidifié la capacité des enquêteurs gouvernementaux à obtenir des fichiers auprès de fournisseurs traitant des données sur le sol étranger.

Dans le même temps, les défenseurs de la protection de la confidentialité se sont opposés à l'échange de données entre les fournisseurs américains et européens. La disposition relative à la sphère de sécurité (Safe Harbour) permettait aux fournisseurs américains de transférer aux États-Unis des données provenant de partenaires de l'UE s'ils s'engageaient à respecter plusieurs principes en matière de protection de la confidentialité. Max Schrems, avocat et défenseur de la protection de la confidentialité, a contesté cette disposition en 2015, ce qui a conduit à son annulation et à son remplacement par l'accord sur le bouclier de protection des données UE-États Unis (EU-US Privacy Shield). M. Schrems a également contesté cette décision, qui a été déclarée invalide en 2020.

Aujourd'hui, l'Union européenne et les États-Unis s'attaquent une troisième fois au problème avec le cadre transatlantique de protection des données. Un projet de décision d'adéquation, qui tente de remplacer la « décision relative au bouclier de protection des données », invalidée par la suite par l'arrêt Schrems II, a été très récemment publié par l'UE.

D'après les premières réactions de Max Schrems, le projet de décision est presque entièrement basé sur le décret connu qui a été rejeté précédemment. Il est probable que l'équipe de Max Schrems contestera cette décision devant les tribunaux européens. Par conséquent, les entreprises des deux côtés de l'Atlantique restent dans le flou quant à la suite des événements, ce qui peut faire stagner les projets de transformation numérique.

M. Phipps recommande aux organisations de mettre en place des contrôles appropriés pour protéger leurs actifs numériques, afin qu'elles puissent détenir leur propre souveraineté en matière de données et accélérer leur passage au cloud, indépendamment des changements géopolitiques.

Cependant, cela peut représenter un défi considérable dans un environnement de cloud multiple et hybride. Près d'une personne sur cinq ayant répondu à l'enquête de Thales a déclaré ne pas savoir où sont stockées toutes ses données. Environ la moitié a déclaré que la gestion de leurs données sensibles dans des environnements de cloud multiple est plus difficile que sur site. Cette situation peut avoir de graves conséquences. L'enquête de Thales a également révélé que 35 % des personnes interrogées ont subi des fuites de données ou des échecs de vérifiabilité de données et d'applications basées sur le cloud au cours de l'année écoulée.

Souveraineté opérationnelle et logicielle

Selon M. Phipps, la deuxième catégorie de souveraineté numérique est opérationnelle. « Il s'agit du cas où vous avez vos données dans le cloud et que vous vous inquiétez d'une menace interne ou d'acteurs malveillants », explique-t-il. « Cela peut être un ingénieur du cloud, mais cela peut aussi être votre propre personnel. » Un employé malhonnête cherchant à obtenir un gain financier personnel pourrait voler vos données, tout comme un travailleur mécontent de votre entreprise, éventuellement à la demande d'un tiers.

La menace pour la souveraineté opérationnelle peut également se présenter sous la forme d'un programme malveillant, d'une application corrompue ou d'un ransomware qui a récupéré les identifiants de connexion d'un utilisateur privilégié afin d'obtenir un accès élargi à des données ou des systèmes sensibles.

Enfin, Thales cite la souveraineté logicielle comme un problème pour les entreprises. « Il s'agit de la possibilité d'exécuter vos charges de travail où vous le souhaitez », déclare M. Phipps.

Les entreprises veulent de plus en plus avoir le choix lorsqu'elles passent au cloud. Elles pourraient vouloir exécuter la plupart de leurs charges de travail avec un fournisseur de cloud spécifique afin d'obtenir de meilleures conditions commerciales, explique-t-il. Mais les régulateurs craignent que, s'il n'y a pas de possibilité de procéder à une sortie contrôlée et rapide de la crise, ces entreprises mettent tous leurs œufs dans le même panier. Les organisations sont encouragées à s'assurer que leurs charges de travail critiques sont sécurisées et transférables, ce qui contribue à garantir la résilience opérationnelle et la continuité des activités en cas de problème.

Par exemple, l'Autorité de régulation prudentielle de la Banque d'Angleterre, qui a succédé à l'Autorité des services financiers, s'est inquiétée de la dépendance des banques à l'égard du cloud computing à partir d'un fournisseur unique. Elle recommande aux institutions de services financiers d'adopter des architectures de cloud multiple afin de répartir les risques et d'éviter le verrouillage des fournisseurs, tandis que la loi sur la résilience opérationnelle numérique aussi appelée DORA (Digital Operational Resilience Act) dans l'UE préconise une approche similaire.

Par conséquent, les banques sont contraintes de partager leurs charges de travail et d'avoir des fournisseurs cloud de secours vers lesquels elles peuvent basculer en cas de panne ou de rupture de la relation.

Protection de la souveraineté numérique en pratique

Thales s'est fait un devoir de répondre à ces diverses exigences en matière de souveraineté. Elle utilise un processus en quatre étapes pour amener ses clients sur un terrain positif où ils se sentent totalement maîtres de leurs données, de leurs opérations et de leurs logiciels.

L'entreprise commence par un processus de découverte. Après tout, on ne peut pas contrôler ce que l'on ne connaît pas. L'entreprise cherche donc à répondre à des questions telles que : où se trouvent nos données et quelles sont-elles ? Dans quelle mesure sont-elles sensibles ?

Selon M. Phipps, de nombreuses organisations ne connaissent pas ces informations de base. Les entreprises génèrent en permanence de nouvelles données et il ne s'agit plus simplement de classer les registres de la base de données dans des champs connus. « De plus en plus, une grande partie des données sensibles générées sont non structurées et apparaissent dans des endroits aléatoires », affirme-t-il. L'adoption grandissante du cloud et les politiques modernes de travail à distance ont contribué à ce que 2,5 trillions d'octets de nouvelles données soient générés chaque jour dans les e-mails, les présentations et les feuilles de calcul, selon certaines estimations. Sans aide extérieure, il est beaucoup plus difficile de localiser les informations sensibles contenues dans ces vastes volumes.

À cette fin, Thales a développé la solution Data Discovery and Classification (DDC), qui recherche des types de données spécifiques en fonction des modèles de conformité auxquels l'organisation s'intéresse. DDC utilise des algorithmes d'apprentissage automatique, ainsi qu'une bibliothèque de référence de modèles prédéfinis de

confidentialité des données et de réglementation, tels que le RGPD, la CCPA, la LGPD, PCI DSS et HIPAA, pour trouver les données sensibles d'intérêt et appliquer une note de risque basée sur les politiques et la conformité du client. DDC peut alors recommander une remédiation manuelle ou l'appliquer automatiquement, ce qui permet de gagner du temps et de minimiser la surface d'attaque.

Protection par chiffrement multicouche

À quoi ressemble cette remédiation ? C'est là qu'intervient la deuxième étape de la méthodologie de Thales, à savoir la protection. Elle se concentre principalement sur le chiffrement multicouche, qu'elle divise en trois types : les données au repos, en transit et en cours d'utilisation.

Comme le souligne M. Phipps, tous les grands fournisseurs de cloud chiffrent par défaut les données au repos. Mais il y a un bémol : nombre d'entre eux ne les chiffrent qu'au niveau du disque. Cela peut empêcher quelqu'un de récupérer les données dans le cas peu probable où il volerait un disque physique dans le centre de données du cloud, mais que se passerait-il s'il détournait le compte d'une personne à distance ? Peu de fournisseurs de cloud, si ce n'est aucun, chiffrent automatiquement les données au-dessus du niveau du disque, par exemple au niveau du fichier, de la base de données ou de l'application, ce qui peut contribuer à atténuer cette menace.

Thales propose des solutions pour chiffrer les données à plusieurs niveaux, y compris les données structurées et non structurées, afin de mettre en place une défense en profondeur. Le chiffrement transparent au niveau des fichiers protège l'ensemble de la base de données pour un surcoût de performance d'environ 2 %, explique M. Phipps. Les clients peuvent appliquer des niveaux de chiffrement plus élevés à des champs spécifiques de la base de données s'ils le souhaitent.

Bien que cela impose un surcoût en matière de performances, cela permet également de renforcer les niveaux de protection là où cela est nécessaire. La sécurité, la conformité et les performances font souvent l'objet de compromis. L'essentiel est d'adopter une approche fondée sur le risque pour s'assurer que la protection appliquée de manière appropriée est basée sur les résultats souhaités par l'entreprise.

En ce qui concerne le chiffrement en transit, TLS est la norme de facto. Toutefois, M. Phipps fait valoir que cela peut souvent s'avérer problématique compte tenu des importants volumes de données que certains fournisseurs traitent dans le cloud. Au lieu de cela, Thales propose un chiffrement à haut débit dans ses produits de chiffreurs réseau, qui, selon M. Phipps, sont plus rapides que TLS et offrent un degré de protection plus élevé.

Thales met également l'accent sur le chiffrement des données en cours d'utilisation, qui permet de lutter contre le sabotage ou l'espionnage pendant le traitement sur le cloud. « Nous avons discuté avec des fournisseurs d'infrastructures critiques, tels que des fournisseurs d'énergie, et ils s'inquiètent de l'exécution de charges de travail sensibles dans le cloud pour des applications critiques en ce qui concerne la sécurité », explique M. Phipps. « Si quelqu'un injecte un programme malveillant dans une puce qui traite des données, il peut effectivement procéder à un déni d'accès et mettre tout le système hors service. »

Pour lutter contre ce phénomène, les fournisseurs du cloud travaillent sur diverses initiatives d'informatique confidentielle. Dans ces services, une partie de la puce devient une enclave sécurisée sous le contrôle du client plutôt que du fournisseur de services du cloud. Microsoft Azure, Google Cloud et AWS proposent tous des offres dans ce domaine.

Maintenir la souveraineté des données dans le cloud

Le troisième pilier du service de souveraineté numérique de Thales concerne le contrôle. Le fait de laisser ces clés de chiffrement dans le cloud les place théoriquement sous le contrôle du fournisseur de services du cloud, ce qui constitue une menace évidente pour la souveraineté du client. Cela rend le client vulnérable aux comportements malveillants ou aux erreurs d'un tiers, comme les propres ingénieurs d'assistance du fournisseur de services du cloud. Les données sont également menacées en cas d'assignation à comparaître d'un État étranger.

La solution à cette menace réside dans la séparation des tâches. La création et le stockage des clés de chiffrement en dehors du cloud, en les séparant de l'endroit où les données sensibles sont stockées, donnent au client un contrôle ultime sur les données. En cas de menace pour les données, le client peut conserver les clés. Comme le fournisseur de services du cloud ne peut pas accéder unilatéralement à ces clés, il ne peut pas être contraint de remettre les données à un tiers.

Certains fournisseurs du cloud ont mis en place des services permettant aux clients de stocker leurs propres clés pour les charges de travail basées sur le cloud, créant ainsi une séparation claire des tâches entre le fournisseur de services du cloud et le client. La gestion externe des clés (EKM) de Google Cloud en est un bon exemple.

Thales a collaboré avec Google Cloud pour aider ses clients à gérer le contrôle de leurs données, de leurs opérations et de leurs logiciels tout en bénéficiant des avantages du cloud computing. En décembre 2020, elles ont travaillé à l'intégration du service CipherTrust Key Broker de Thales avec l'EKM de Google Cloud. Cela permet aux clients de générer leurs clés de chiffrement pour le service cloud de Google tout en conservant les clés en dehors de l'environnement de Google Cloud.

Depuis, les deux entreprises ont étendu leur partenariat à d'autres services. En juin 2021, CipherTrust Manager et le produit SafeNet Trusted Access de Thales ont été intégrés pour prendre en charge le chiffrement côté client du service Workspace de Google, par exemple. Les organisations peuvent ainsi chiffrer les données de Google Drive à l'aide de leurs propres clés.

L'année dernière, elles ont également collaboré à la mise en place d'une plateforme basée sur le cloud qui répond au label Trusted Cloud du gouvernement français. Cela oblige les fournisseurs de services du cloud à héberger leurs serveurs en France et à n'autoriser que les fournisseurs européens à exploiter ces serveurs en utilisant les citoyens européens tout en limitant les transferts de données vers d'autres pays. En outre, cela nécessite de définir une série d'exigences juridiques, physiques, opérationnelles et techniques.

En attendant, la co-entreprise détenue majoritairement par Thales avec Google Cloud, S3NS, permet déjà aux clients de Google Cloud en France de restreindre l'accès aux sites de l'UE, à l'aide de ses propres services de gestion des clés. S3NS gère les clés de haut niveau, les identités et les racines de confiance, ainsi que la vérification des mises à jour de Google Cloud et l'examen du code source. S3NS développe également un service conforme au Trusted Cloud, dont la sortie est prévue pour 2024.

L'unification des opérations et de la gestion des clés dans le cloud, tout en gardant les clés sous le contrôle du client, résout l'un des plus gros problèmes de la sécurité dans le cloud : la complexité de la gestion des clés. L'enquête de Thales a révélé que 57 % des entreprises utilisent au moins cinq solutions distinctes de gestion des clés, ce qui accroît la complexité et le coût de la gestion du chiffrement des données. Le regroupement et la simplification de cette gestion des clés deviendront de plus en plus critiques à mesure que les entreprises gèrent des données sensibles dans un environnement de plus en plus distribué.

Contrôler la souveraineté numérique dans le temps

Alors que les entreprises continuent d'étendre leurs numérisations dans des environnements de cloud multiples et hybrides complexes, elles ont besoin d'un moyen de garder une certaine visibilité. C'est là qu'intervient la dernière partie du processus de souveraineté numérique de Thales : le suivi. La plateforme CipherTrust de l'entreprise, actuellement disponible en tant que produit sur site mais bientôt lancée en tant que service, offre une vue unique de la souveraineté numérique sur l'ensemble de leurs outils et processus dans des environnements de cloud multiples et cloud hybrides. Le système permet d'accéder à une gamme de produits tiers en plus de DDC de Thales.

Les principes et les pratiques en matière de souveraineté numérique ne feront que se complexifier au fil du temps, estime M. Phipps. C'est pourquoi il insiste sur les avantages de l'intégration de la protection de la confidentialité dès la conception dans les architectures de cloud hybrides et multiples. Phipps insiste également sur la nécessité d'établir des relations humaines fondées sur la confiance et l'empathie, afin de maximiser l'expérience du client.

« La technologie seule, sans les bonnes relations avec les conseillers et les fournisseurs, ne permettra probablement pas au client de mieux comprendre la marche à suivre », conclut-il. C'est là un casse-tête difficile à résoudre dont seules une expertise externe et une approche collaborative peuvent venir à bout.