Construire un écosystème de confiance pour le Cloud

Pour une DSI confiante dans les usages Cloud et force de proposition auprès des métiers

Alexis Quentrec

Master Spécialisé ISEP - “Expert Cloud Computing et SaaS”
Promotion 2015-2016

V1.1

Remerciements

J'adresse mes remerciements aux personnes qui m'ont aidé dans la réalisation de ce mémoire.

En premier lieu, je remercie M. Louis Naugès, expert référent et évangéliste Cloud renommé. En tant que tuteur, il m'a guidé dans mon travail et a su m'orienter lorsque je m'étais égaré.

Je remercie aussi M. Antoine Jacquier, fondateur du cabinet Nuageo, qui m'a poussé vers cette formation et m'a accompagné tout autant pendant les cours, pendant la mission en entreprise, et pendant la rédaction de ce mémoire.
C'est aussi l'occasion de remercier M. Clément Marche, collègue de Nuageo et ancien étudiant de ce Master, qui m'a partagé son expérience de cette formation.

Je tiens à remercier l'ISEP de proposer cette formation, qui fournit un cadre propice aux échanges bienveillants entre les enseignants et les étudiants.
Je souhaite remercier les intervenants qui ont partagé leurs expertises tout au long de la formation, et surtout pour leur disponibilité lors des échanges pendant et en dehors des sessions de formation.
Je souhaite aussi remercier mes collègues de formation, qui m'ont permis d'acquérir une nouvelle façon de concevoir l'informatique et le monde professionnel, mais qui ont surtout été une formidable source de motivation et de plaisir pendant cette année.

Enfin, je remercie mes proches qui m'ont supporté lors de cette année d'étude, autant dans les bons moments que les moins bons.

Table des matières

Executive summary

Le Cloud est un mode de consommation de l'informatique qui s'impose petit à petit. Pour autant, les entreprises hésitent à sauter le pas à cause d'un manque de confiance dans ce type de services.

L'urgence est pourtant réelle : les DSI [1]doivent gérer des infrastructures informatiques importantes, en délivrant la valeur ajoutée attendue sur les applications coeur de métier, tout en gérant des applications sur lesquelles la DSI génère peu de valeur. Sur ce type d'applications Support, transverses et à destination de l'ensemble des utilisateurs, les services SaaS [2]représentent une réponse idéale pour la DSI de se décharger de la gestion quotidienne de services chronophages pour se concentrer sur le coeur de ses missions.

La pertinence de ces solutions est illustrée par le phénomène du Shadow IT[3] : les directions métiers se tournent volontairement vers des usages informatiques de l'ombre, disponibles sous forme de SaaS, au détriment des services traditionnels proposés par la DSI et en faisant peser un risque fort sur la sécurité et la confidentialité des données de l'entreprise.

Pour cela, la DSI doit disposer d'un écosystème de confiance Cloud qui sécurise la consommation de services SaaS : grâce à cet ensemble technique, la DSI peut transférer rapidement et efficacement ces usages vers le Cloud[4], et se concentrer exclusivement sur ses missions principales.

L'écosystème des fournisseurs est suffisamment mature pour proposer des services autour de la sécurité des données, du réseau, des terminaux, mais aussi de l'authentification et de l'intégration. Enfin, un élément essentiel est la détection des usages non autorisés.

Chaque entreprise peut construire l'écosystème qui lui est adapté selon ses besoins.

Ces besoins doivent être adaptés selon l'industrie de l'entreprise, le type d'utilisateurs et l'activité qu'ils effectuent au sein de l'entreprise. Pour cela, il est possible d'utiliser une matrice d'aide à la définition des exigences de confiance

Enfin, l'écosystème de confiance doit être testé en condition réelle par les utilisateurs finaux avant un déploiement généralisé : une fois cette validation effectuée, la DSI pourra proposer des services SaaS en toute confiance.

[1] Direction des Systèmes d'Information
[2] Software-as-a-Service : application disponible en ligne, à la demande
[3] Informatique de l'ombre : désigne l'utilisation non autorisée par la DSI de logiciels ou services informatique
[4] Cloud : fait référence au Cloud Computing, ou l'informatique en nuage - un mode de distribution de ressources informatiques virtualisées à la demande par l'intermédiaire du réseau internet

La réponse technique à la confiance ne doit pas faire oublier qu'il faut dépasser la technique : la question de la confiance se traite aussi par les certifications des solutions, et par une organisation transversale dans l'entreprise.

C'est par une gouvernance mêlant les métiers et la DSI que l'usage des services SaaS pourra s'imposer comme le nouveau mode d'utilisation de l'informatique.

Introduction

Les DSI sont à la croisée des chemins.

Aujourd'hui, elles sont régulièrement remises en question dans leurs attributions, car elles sont perçues comme coûteuses et ne délivrant pas une valeur ajoutée clairement identifiée aux utilisateurs finaux.

Du fait des nouvelles tendances de l'informatique, les SMAC [5], les usages ont changé, et les innovations ont rapidement dépassé le cadre des compétences de la DSI, ce qui a entraîné une perte de confiance des utilisateurs dans la DSI.

Cette situation est d'autant plus paradoxale que les DSI ont aujourd'hui à leur disposition des outils performants, peu coûteux, et répondant parfaitement à leurs usages.

Grâce au Cloud Computing, il est possible de construire un système d'information performant et innovant, capable d'adresser les besoins des utilisateurs.

En reprenant le modèle B I S de Monsieur Naugès, on peut décomposer un système d'information en 3 briques :

- **B** : Business. Il s'agit des applications « cœur de métier » de l'entreprise, qui ont vocation à être exploitées en interne ou sur un service Cloud de type PaaS[6].
- **I** : Infrastructure. Cette dénomination couvre les différents éléments constitutifs de l'infrastructure du SI de l'entreprise, tels qu'on peut les retrouver notamment dans les services Cloud IaaS[7].
- **S** : Support. Enfin, cette catégorie couvre les services applicatifs mis à disposition des utilisateurs finaux, comme les outils bureautiques, la messagerie, le CRM[8]…

Aujourd'hui, les DSI prennent en charge la gestion intégrale de ces 3 briques; or, elles ne disposent plus des moyens leur permettant de gérer l'intégralité de ces services de façon satisfaisante pour les utilisateurs.

Les applications Support incarnent naturellement la brique sur laquelle les DSI doivent se concentrer pour le Cloud : ces applications, généralistes, ne sont pas favorables à générer une forte valeur ajoutée pour les équipes SI.

[5] Social Mobile Analytics Cloud : les 4 socles technologiques qui révolutionnent les usages informatiques
[6] Platform-as-a-Service : un service proposant un environnement à la demande pour le développement d'applications
[7] Infrastructure-as-a-Service : un service proposant des ressources informatiques (type CPU, RAM, stockage, réseau,...) virtuelles à la demande
[8] Customer Relationship Management : outil de gestion de la relation client

En libérant les équipes SI de la gestion des applications Support, elles peuvent se concentrer entièrement sur les briques critiques Business et Infrastructure du SI.

Or, aujourd'hui, la DSI fait preuve de défiance envers le Cloud : perçu comme un cheval de Troie et vecteur de failles de sécurité, elles sont réticentes à sauter le pas.
L'objectif poursuivi par ce mémoire est donc de donner les clés de la confiance dans le Cloud à la DSI, pour permettre la généralisation du Cloud pour les applications Support.

Sous l'impulsion du Shadow IT, un ensemble de solutions visant à construire la confiance dans le Cloud ont été développées. Elles doivent maintenant être orchestrées pour permettre à la DSI de construire son propre écosystème de confiance Cloud qui lui permettra de systématiser le recours au Cloud pour les applications Support.

I - L'opportunité pour la DSI sous la menace du SaaS

Le Cloud s'impose comme l'alternative la plus pertinente pour la DSI de délivrer de la valeur ajoutée aux métiers sur des applications Support sur lesquelles elles disposent de peu d'expertise.

Le catalogue de services disponibles dans le Cloud, et plus particulièrement sous la forme du SaaS, est conséquent et de nature à satisfaire les besoins des utilisateurs finaux.

L'une des illustrations les plus flagrantes de ce phénomène est le Shadow IT qui, sous l'impulsion des utilisateurs finaux, court-circuite totalement la DSI dans ses prérogatives en faisant courir un risque fort sur la sécurité des données de l'entreprise.

A ce titre, la mise en oeuvre d'un écosystème de confiance Cloud au sein de la DSI s'impose comme un impératif pour permettre à la DSI de se concentrer sur ses attributions premières, à savoir délivrer la valeur ajoutée du SI sur l'infrastructure et les applications coeur de métier.

Pour cela, elle doit capitaliser sur le catalogue de services disponibles, et endiguer le Shadow IT.

A - La puissance du Cloud au service de la DSI

Le Cloud Computing offre une nouvelle façon de consommer l'informatique, dont la DSI doit tirer partie : dans un premier temps, il s'agit d'une opportunité de se recentrer sur la génération de valeur ajoutée. Dans un second temps, il s'agit aussi d'un puissant levier d'optimisation.

1 - Un recentrement stratégique sur la valeur ajoutée grâce à un immense catalogue de services

Les services de la DSI sont architecturées autour des trois briques Business - Infrastructure - Support.

Les briques Business et Infrastructure sont les éléments traditionnels de la DSI, autour desquels les équipes techniques de la DSI ont développé leur expertise. Il s'agit aujourd'hui des éléments majeurs autour desquels la DSI délivre sa pleine valeur ajoutée.

Pour autant, la DSI est aussi responsable de la brique Support, qui consiste principalement en l'exploitation de services sur lesquels l'expertise de la DSI est moins prononcée, voire souvent absente.

La DSI a développé une expertise certaine sur le maintien et le développement du SI existant; que ce soit par des équipes techniques dédiées au développement ou au réseau, il est indiscutable que la DSI est au centre des évolutions techniques du SI de l'entreprise.

De plus, de nouvelles contraintes pèsent sur les entreprises, et donc sur la DSI : les priorités sont mises sur la recherche de valeur ajoutée, mais de façon rationnelle : les investissements lourds dont les bénéfices sont aléatoires sont fermement encadrés et limités.

Cela a pour conséquence directe une diminution de l'échelle des projets informatiques qui, s'ils n'ont pas un impact direct bénéfique sur la rentabilité de l'entreprise ou sa capacité à mieux adresser son marché, ne sont pas validés. Le patrimoine informatique est donc maintenu opérationnel, souvent rationalisé, mais rarement étendu : les investissements privilégiés sont ceux ayant trait au coeur de métier de l'entreprise, et non pas ceux liés à une fonction support (mais néanmoins critique) de l'entreprise.

Cette tendance se manifeste particulièrement auprès des entreprises utilisatrices de services ERP extensifs (tels que SAP, Oracle ou SAGE) : le montant des évolutions vers les nouvelles versions de ces applications se révèle trop important pour un bénéfice qui n'est pas toujours identifié, ce qui incite ces entreprises à conserver un parc d'applications vieillissantes, mais pertinentes au vu du rapport coût/fonctionnalités.

Ces investissements structurants sont donc amenés à s'amenuiser, pour évoluer vers des investissements plus localisés et plus tactiques : plutôt que des projets longs et complexes à mener, les entreprises et les DSI se dirigent vers des chantiers tactiques, qui répondent plus rapidement à une problématique; ainsi, la migration d'une solution CRM sur 6 mois est favorisée à la migration d'un système de production industrielle sur plusieurs années.

Une alternative à cette tendance est donc le choix de solutions Cloud pour les applications Support : l'utilisation de ces services n'implique pas, a priori, d'investissements lourds en infrastructure et coûteux en temps et ne provoque pas l'immobilisation de capitaux. De plus, l'utilisation de services Cloud a de nombreux bénéfices pour les équipes techniques, en réduisant le temps consacré à la maintenance du matériel pour se focaliser sur la maintenance des systèmes applicatifs et sur la valeur ajoutée délivrée aux opérationnels.

AngelList, le site de référence sur les startups et les business angels, dénombre plus de 10.700 startups proposant un service SaaS; GetApp.com, une place de marché américaine de référence pour le Saas compte plus de 4.700 services SaaS. Pour Synergy Research Group, les acteurs majeurs du marché SaaS en 2015 ont été Salesforce, Microsoft, Adobe et SAP avec une part de marché combinée d'approximativement 35%.

En 2015, le marché des services SaaS a connu une croissance supérieure à 15% selon Gartner; en 2016, le marché des services SaaS atteindra un volume de 37.7milliards de dollars.

L'offre de services SaaS est donc vaste, et il est facile de s'y perdre. Devant le nombre de services disponibles, et l'impossibilité de tous les référencer de façon exhaustive, il faut être lucide : il existe probablement un service pour chaque besoin. Dans le pire des cas, il est possible qu'il existe plusieurs services à faire coexister pour répondre à l'ensemble du besoin identifié.

L'offre est rendue d'autant plus complexe à déchiffrer que les services sont proposés aussi bien par des éditeurs établis de l'informatique traditionnels que par de nouveaux acteurs dont l'historique est moins connu, et dont la stabilité financière est moins assurée, malgré un service Cloud qui peut s'avérer plus intéressant pour le client.

Ainsi, le choix de solutions Cloud doit se faire en toute connaissance de cause et en capitalisant sur les expertises existantes : loin de remplacer le patrimoine historique, les services Cloud doivent compléter les capacités existantes sur des points particuliers où la DSI n'a pas vocation à délivrer une valeur ajoutée.

Car le coeur des évolutions futures du SI des entreprises n'est pas la gestion extensive de tous les éléments qui le constituent, mais bien la façon de délivrer la valeur ajoutée pertinente aux utilisateurs finaux, avec un coût raisonnable.

2 - La puissance du Cloud comme vecteur d'optimisations

Au-delà de l'échelle des projets SI, il est une autre opportunité qui se présente aux DSI : l'amélioration des performances.

Les futurs SI se dessinent, et seront très probablement hybrides : mêlant une partie sur site et une partie dans les nuages.

Si les projets d'infrastructures sur site vont se réduire pour se concentrer autour de projets toujours plus localisés et spécialisés vers le coeur de métier de l'entreprise, la conséquence est que le parc matériel et logiciel existant sera soit conservé, soit migré vers le Cloud, soit redéployé.

Ces deux dernières hypothèses présentent les avantages les plus importants pour les entreprises et pour les utilisateurs finaux : les ressources libérées et redéployées seront ainsi mises à profit de l'optimisation de l'infrastructure de l'entreprise.

Dans le cadre de la migration vers le Cloud, les ressources seront ainsi disponibles selon la demande, avec un mode de facturation et d'utilisation permettant d'accéder à de nouveaux leviers d'optimisation.

Ces leviers sont intimement imbriqués : les optimisations pourront être d'ordre matérielles et financières.

Ainsi, en optimisant l'utilisation de ressources informatiques grâce à la virtualisation d'abord, puis la mutualisation des ressources, et enfin par l'utilisation de ressources externalisée à la demande, la DSI peut accélérer sa performance budgétaire par un équilibre entre la commande et l'utilisation de ressources Cloud et l'utilisation faite des services par les utilisateurs finaux.

De façon incidente, l'optimisation financière a aussi lieu par une rationalisation des coûts électriques : le matériel qui n'est plus hébergé sur le site de l'entreprise ne génère plus de consommation électrique, ni ne nécessite de refroidissement.

De la même manière, le matériel non utilisé ne demande plus d'être inclus dans les contrats de maintenance annuels, ce qui libère des capacités budgétaires pour d'autres postes.

Enfin, l'optimisation peut aussi avoir lieu par le biais de l'augmentation des performances : la réallocation de machines physiques et virtuelles internes jusque là dédiée à des services nécessaires mais à faible valeur ajoutée pour l'entreprise (comme la messagerie) peut permettre d'améliorer les performances d'applications métiers critiques en apportant un complément de puissance, si l'augmentation du volume d'utilisateurs ou du volume à traiter le rend nécessaire notamment.

A ce titre, le Cloud devient d'abord un relais interne à la DSI pour optimiser son budget et les évolutions du SI; et il s'agit surtout d'un relais pour susciter la confiance des utilisateurs dans la capacité de la DSI à les accompagner.

B - Un contournement de la DSI

1 - La prise de pouvoir de l'informatique de l'ombre

Aujourd'hui, la principale menace pesant sur le SI traditionnel provient du Shadow IT, c'est à dire l'utilisation d'applications non autorisées par la DSI dans le cadre professionnel. Les principaux dangers liés au Shadow IT portent notamment sur la compromission de la confidentialité des données de l'entreprise, avec de fortes possibilités de rendre ces données accessibles à des assaillants à partir des terminaux personnels des utilisateurs, qui sont le plus souvent moins bien protégés que les terminaux de l'entreprise.

A travers l'utilisation de services non autorisés par la DSI, c'est surtout une remise en question de la place de cette dernière dans la proposition des services adéquats pour les utilisateurs : en effet, la consumérisation des services informatiques a entraîné le glissement de nombreux usages de la sphère privée vers la sphère professionnelle, ce qui est facilité notamment par les applications mobiles et cloud.

Ainsi, le recours au Shadow IT traduit en filigrane une remise en cause des choix effectués par la DSI dans son offre de service, et plus particulièrement sa capacité à dialoguer avec les utilisateurs finaux pour comprendre et s'approprier leurs besoins : le plus souvent, les utilisateurs se tournent vers des services intuitifs et plus simples d'utilisation dans le but de pouvoir améliorer leur productivité, par dépit de ne pas avoir trouvé la solution adéquate parmi le choix proposé par la DSI.
C'est par exemple le constat émis par la DSI du groupe Saint-Gobain, et qui l'a poussée à mettre les usages Cloud au coeur de sa stratégie[9].

En d'autres termes, les utilisateurs finaux ont identifié des usages critiques pour accomplir leurs missions, mais se sont heurtés à un manque de disponibilité du service adéquat.
En effet, en favorisant la vision usage au détriment de la vision application, l'utilisateur s'est placé dans une approche fondamentalement différente de l'approche traditionnelle de la DSI, faisant apparaître un fossé difficile à combler rapidement considérant les expertises existantes au sein des équipes SI et des stratégies déployées par ces équipes pour l'évolution du patrimoine informatique de l'entreprise.

2 - Un usage plébiscité en danger

Aujourd'hui, il est estimé que le Shadow IT représente 15% des dépenses IT dans les entreprises; pour autant, ces estimations sont basses, et des études montrent que les métiers ont recours entre 15 et 20 fois plus aux applications de l'ombre que ce que la DSI avait identifié[10]. 81% des utilisateurs métiers admettent utiliser des applications non approuvées par la DSI...et la proportion monte à 83% pour les employés de la DSI.[11]

Ce phénomène est d'autant plus renforcé que les éditeurs sont en position de force : ces derniers sont directement en contact avec les responsables métiers pour leur

9 http://www.larevuedudigital.com/2016/03/26/le-shadow-it-createur-de-solution-entre-la-dsi-et-le-metier-chez-saint-gobain/
10 http://www.cio.com/article/2968281/cio-role/cios-vastly-underestimate-extent-of-shadow-it.html
11 http://www.cioinsight.com/security/slideshows/shadow-its-growing-footprint.html

proposer leurs services, en contournant ouvertement la DSI au nom du principe de réactivité.

Le fonctionnement budgétaire des entreprises est un terreau fertile à ce développement : les dépenses d'investissement se réduisent de par l'immobilisation des liquidités de l'entreprise qu'elles entraînent, alors que les dépenses de fonctionnement sont favorisées pour leur flexibilité et leur volumétrie variable.

Le SaaS, avec son fonctionnement et sa tarification à la demande, permet aux directions métiers d'accéder rapidement et simplement à des outils puissants, au contact direct des éditeurs.

78% des managers métiers font aujourd'hui recours au Shadow IT, et cette tendance va s'accentuer si la DSI ne réagit pas.

En effet, aujourd'hui, le Shadow IT est considéré comme essentiel à l'activité par 77% des managers. On peut citer le besoin de réactivité et de flexibilité comme les leviers essentiels d'adoption de ces services.[12]

Cependant, les mentalités évoluent et certaines DSI ont entamé leur transformation pour faire du Shadow IT leur allié : chez Saint Gobain[13], l'usage de Shadow IT est perçu comme un besoin à adresser, et une opportunité pour la DSI d'accompagner le métier vers un nouvel usage. Cette entreprise a par ailleurs adopté une stratégie IT ouvertement pro-Cloud : ses services utilisent déjà largement les services d'infrastructures proposés par Amazon Web Services[14], ou encore les plateformes de Cornerstone [15]pour ses besoins de formation.

[12] http://www.silicon.fr/shadow-it-dsi-ministere-non-154198.html

[13] http://www.larevuedudigital.com/2016/03/26/le-shadow-it-createur-de-solution-entre-la-dsi-et-le-metier-chez-saint-gobain/

[14] http://www.lemagit.fr/etude/Saint-Gobain-elargit-sa-strategie-multi-Cloud

[15] https://www.cornerstoneondemand.fr/company/news/press-releases/saint-gobain-s%e2%80%99appuie-sur-le-cloud-de-cornerstone-ondemand-pour-ouvrir-ses

II - La nécessité d'un écosystème de confiance Cloud pour sécuriser l'entreprise et les utilisateurs

La meilleure façon de lutter contre le Shadow IT est d'utiliser les mêmes armes : le Cloud, et plus particulièrement les services SaaS.

Pour la DSI, la menace est forte : il s'agit d'une attaque claire sur ses prérogatives traditionnelles, et par laquelle elle est remise en question. Il existe de forts risques pour l'entreprise à ne pas adresser cette menace.

Pour cela, la façon la plus efficace est pour la DSI de mettre à disposition des métiers des services SaaS performants qu'ils peuvent consommer sans arrière pensée. Pour arriver à cet état de l'art, la DSI se doit de disposer d'un écosystème technique qui lui permette de susciter la confiance dans les usages Cloud.

A - Une menace réelle et sérieuse

Le Shadow IT fait peser un risque avéré sur l'intégrité du SI des entreprises; pour autant, cet usage non autorisé est l'indication d'une réelle opportunité pour la DSI.

1 - Un risque trop important

Malgré l'utilisation répandue du Shadow IT, les managers métiers reconnaissent le danger de son utilisation, et plus de 70% d'entre eux sont prêts à abandonner cette pratique lorsque la DSI propose un service adapté.

La plupart des managers métiers ne sont pas formés aux enjeux SI, et à ce titre n'ont pas conscience des risques qui pèsent sur l'entreprise en utilisant des outils de l'ombre.

Il existe de réelles menaces sur la confidentialité des données : en rendant les données de l'entreprise accessible en dehors du contexte de celle-ci, les utilisateurs ne bénéficient plus des politiques de sécurité que la DSI a mis en place pour garantir la sécurité des données. Les utilisateurs engagent donc leur propre responsabilité lorsque les données sont exploitées en dehors du cadre prévu par la DSI, avec des conséquences réelles pour leur entreprise.

De même, un véritable enjeu existe autour de la localisation des données et leur accès par des tiers non autorisés, y compris par les fournisseurs Cloud : si les DSI ont conscience de cet enjeu avec les conséquences juridiques qui sont liées, il n'en est pas de même pour les utilisateurs qui, en majorité, ignorent tout de la localisation des services Cloud (56%).

Un autre problème qui découle de l'utilisation du Shadow IT est le morcellement des référentiels de données. Si l'une des missions de la DSI est la garantie de la cohérence des données de l'entreprise, l'utilisation de données de l'entreprise en dehors du cadre prévu par la DSI provoque une fragmentation des données, et donc une diminution de la qualité de ces dernières.

Cet enjeu est crucial : la cohérence des données garantit que les politiques de sécurité et de confidentialité de ces dernières sont respectées. Ainsi, des politiques particulières sont mises en place pour garantir la confidentialité des données personnelles ou de santé par exemple; en exploitant des données en dehors de ces politiques d'utilisation, l'utilisateur expose involontairement l'entreprise à des risques politiques et juridiques importants.

Après les scandales Sony [16] ou PRISM[17], une véritable prise de conscience de l'ensemble de l'entreprise a eu lieu autour des problèmes de sécurité du système d'information, et plus particulièrement autour des différents vecteurs d'attaque.

Le recours au Shadow IT est perçu comme un nouveau vecteur d'attaque. L'utilisateur expose des informations personnelles qui peuvent être détournées pour générer un accès au sein de l'entreprise grâce au *social engineering*. Comme l'utilisateur n'est pas familiarisé aux enjeux IT, il ne dispose pas forcément des réflexes et des outils pour sélectionner un service Cloud sécurisé et confidentiel : la possibilité d'utiliser un service frauduleux est donc réelle.

Si la sécurisation traditionnelle du SI est déjà assurée par la DSI, l'émergence du Shadow IT impose de nouvelles responsabilités à la DSI sur des outils qu'elle ne maîtrise pas.

La réponse naturelle est l'interdiction stricte de ces outils; mais cette politique est peu efficace et mal perçue des utilisateurs : 39% des utilisateurs d'applications SaaS ne sont pas bloqués par ces mesures, 18% des utilisateurs sont frustrés car leurs tâches sont rendues compliquées par ces mesures, et 24% des utilisateurs revendiquent que les applications de l'ombre sont plus efficaces que les outils que la DSI met à leur disposition.

Des solutions existent : le Shadow IT concerne la révolution de l'usage, et de la nouvelle approche à mettre en place pour satisfaire des utilisateurs toujours plus pragmatiques et autonomes face à l'informatique.

Les utilisateurs se focalisent non pas sur des outils précis, mais sur un besoin qui permet d'améliorer la productivité : les premiers cas médiatisés de l'utilisation de Dropbox en entreprise mettent en avant la nécessité pour les utilisateurs d'accéder aux documents en dehors du lieu de travail afin de pouvoir continuer à travailler; cela

[16] https://fr.wikipedia.org/wiki/Piratage_de_Sony_Pictures_Entertainment
[17] http://www.lesechos.fr/tech-medias/dossiers/affaire_snowden_fbi_nsa/index.php

sous-entend que les outils mis à disposition ne satisfont pas ce besoin et/ou sont trop complexes à utiliser.

Cette situation met aussi en avant un besoin de sensibilisation des utilisateurs quant aux problématiques SI, c'est à dire la cohérence et la sécurité des données de l'entreprise; or le Shadow IT fait planer une menace forte sur ces éléments dont la DSI est garante.

La DSI doit se transformer pour accompagner des utilisateurs finaux dans l'évolution de leurs usages; les utilisateurs finaux doivent aussi transformer leur fonctionnement pour intégrer cette nouvelle responsabilité.

Pour cela, un travail préparatoire commun entre la DSI et la population des utilisateurs finaux doit avoir lieu, et doit favoriser l'émergence d'un véritable climat de confiance entre les deux mondes, avec pour objectif de systématiser un fonctionnement coopératif entre la DSI et les utilisateurs finaux pour le choix des évolutions du système d'information de l'entreprise.

Ce fonctionnement en commun est la clé de voûte de l'organisation de la DSI en tant que centre de service : le fonctionnement en tandem autour d'objectifs communs, avec une méthodologie clairement identifiée et validée par les deux parties doit permettre l'émergence d'une vision de groupe sur l'utilisation des outils informatiques, et plus particulièrement sur la manière dont ces outils permettent aux utilisateurs d'être plus efficaces et innovants.

Selon le même principe, ce fonctionnement rapproché permet de créer une meilleure adhésion des utilisateurs aux outils : ces derniers sont validés par les utilisateurs finaux, qui portent la responsabilité de leur utilisation et de leur adéquation avec les besoins métiers ressentis.

Le rôle de la DSI se transforme alors en celui de conseil, permettant de pousser la réflexion des utilisateurs finaux au-delà d'un problème immédiat; l'objectif étant de mettre en avant l'expertise de la DSI dans sa capacité à gérer le système d'information dans la durée et sa compétence dans la compréhension des besoins des utilisateurs.

Un fonctionnement bicéphale est nécessaire : la DSI et les métiers doivent échanger et élaborer ensemble le socle d'applications Support Cloud qui serviront de colonne vertébrale à l'entreprise.

Si les métiers apportent leur connaissance des besoins et des fonctionnalités qui doivent être satisfaites, la DSI est elle garante des aspects techniques; pour favoriser les usages Cloud, la DSI doit construire un écosystème technique lui offrant l'assurance d'une utilisation maîtrisée des outils Cloud par rapport au SI existant.

2 - Un écosystème à construire

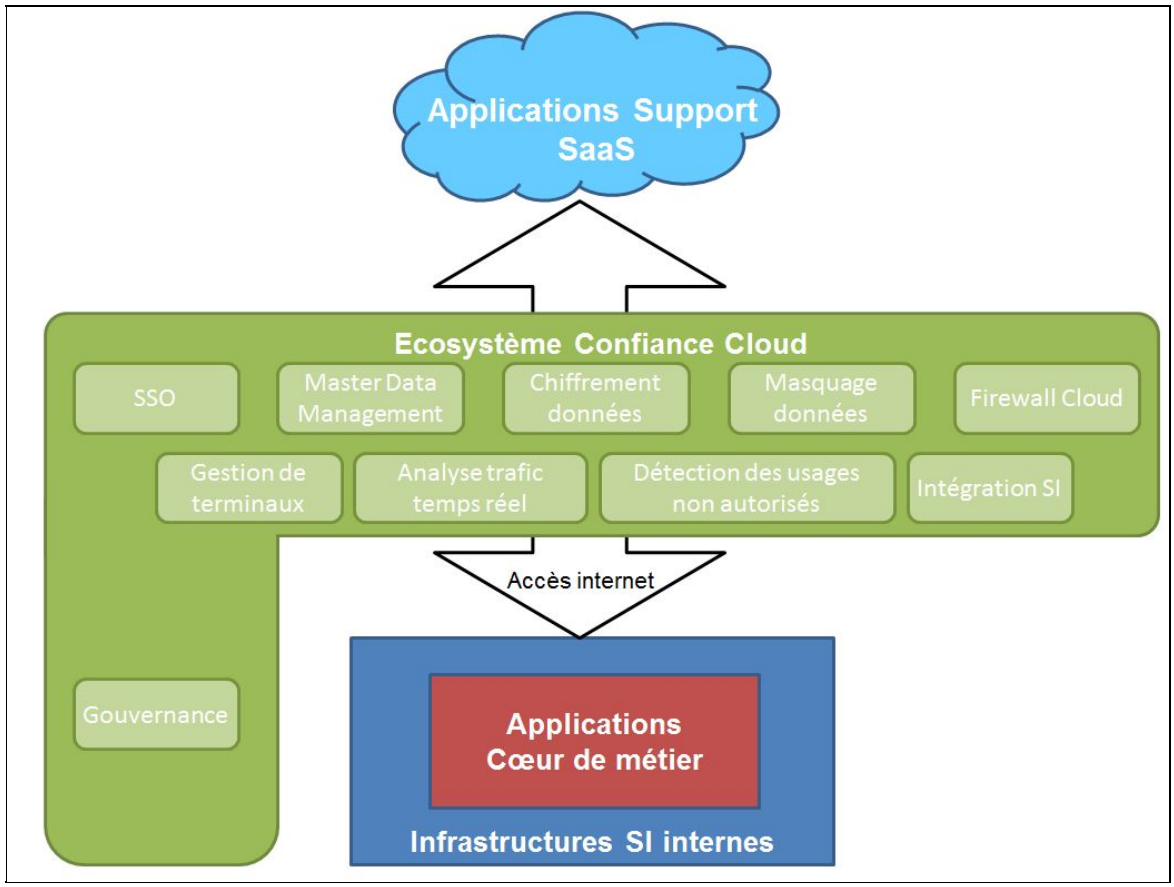
Le principal facteur d'effroi n'est pas tant le manque de sécurité du Cloud, mais bien le manque de maîtrise sur les services : de par la nature des services Cloud, la DSI n'est plus maître de l'exploitation des services, et ne dispose plus du pouvoir sur les mises à jour par exemple.

Cette caractéristique irrévocable du Cloud doit être acceptée : il s'agit d'une formidable opportunité pour la DSI de se consacrer à des tâches à valeur ajoutée.

Les DSI mettent en avant un manque de sécurité et de confidentialité des solutions Cloud pour ne pas les considérer. Or, comme pour les services traditionnels, des solutions existent pour pallier à ces manquements présumés.

En créant un écosystème de confiance, à savoir un ensemble de services visant à garantir la sécurité et la confidentialité des données, la DSI se dote d'une arme imparable pour accepter les services Cloud en son sein, et donner aux métiers l'accès à l'innovation qu'ils recherchent par le Shadow IT tout en se préservant des inconvénients de ce dernier.

En reprenant le modèle B I S, il est possible d'ajouter un élément de Confiance Cloud qui s'insère dans le modèle B I S de la manière suivante :



Gouvernance

Une gouvernance particulière doit régir l'utilisation systématique de services Cloud pour les applications Support. Elle doit s'attacher à décrire le type d'applications concernées, ainsi que les processus liés à leur utilisation.

Une structure de pilotage, avec des indicateurs spécifiques et dédiés, doit être mise en place afin de garantir l'utilisation des services Cloud dans le contexte autorisé par le SI

Cette gouvernance doit aussi régir les relations avec les fournisseurs, en délimitant un périmètre clair de fonctionnalités et de caractéristiques des applications Support.

Des contraintes claires sur la localisation des données, leur traitement, mais aussi les interactions avec le SI de l'entreprise devront être émises afin de guider les processus de sélection et d'utilisation des services Cloud.

Pour piloter la gouvernance liée aux usages Cloud, il sera déterminant de suivre la satisfaction des utilisateurs en systématisant les retours opérationnels : c'est un indicateur incontournable de la qualité de service perçue par les utilisateurs, et donc des axes d'améliorations sur lesquels travailler avec les fournisseurs.

Sécurité

Sécurité des données

Les données sont devenues le nerf de la guerre pour les entreprises. Avec les différents scandales sur la fuite de données, ou la révélation de données confidentielles (Sony, PRISM), les entreprises cherchent de plus en plus à sécuriser leur patrimoine de données.

Un premier pas consiste à mettre en place un ensemble de mesure pour prévenir de la perte de données (Data Loss Prevention). Des outils tels que des firewalls, des détecteurs d'intrusion ou les antivirus doivent être déployés pour prévenir des intentions malveillantes.

En parallèle de ces outils devenus standards, des éléments plus spécialisés dédiés à l'analyse en temps réel des accès aux données, des pièges (honeypots), ou de protection de copie des données doivent être considérés pour sécuriser les données de l'entreprise.

Le chiffrement des données permet, en complément de la gestion des droits d'accès utilisateurs, de rendre les données illisibles à toute personne ou toute application non autorisée.

A défaut d'un chiffrement systématique, un masquage des données est possible : au lieu de rendre la donnée illisible, le masquage rend la donnée non identifiable et anonyme. Moins coûteux que le chiffrement tant en termes de puissance de calcul

que financier,le masquage est une solution efficace dans le cadre de traitement de données personnelle.

En systématisant l'utilisation de ces solutions, la DSI peut se prémunir des impacts négatifs liés aux attaques de pirates informatiques.

Sécurité réseau

Le Cloud se caractérise par un accès à des services par l'intermédiaire d'Internet. A ce titre, il est indispensable de sécuriser et de fiabiliser les accès réseau pour offrir une utilisation sûre des services Cloud.

Avec l'évolution des moyens d'attaques, disposer de moyens techniques préventifs efficaces et à jour est un impératif.

L'utilisation d'un firewall Cloud peut se révéler un atout dans la construction d'une plateforme de confiance : le recours à un service Cloud pour la sécurité permet ainsi la garantie d'une disponibilité importante du service, ainsi qu'une mise à jour en continu contre les différents types d'intrusion.

Enfin, le fonctionnement même du Cloud requiert la connexion réseau : en recourant à un "réseau à la demande" (Network as a Service), la DSI s'offre la flexibilité d'une bande passante à la demande pour offrir la capacité réseau nécessaire pour garantir des usages Cloud qui répondent aux besoins des utilisateurs, avec la possibilité d'optimiser ces besoins réseaux selon le type d'usage.

Gestion des terminaux d'accès

Avec l'adoption des smartphones, des tablettes, et des ordinateurs portables, la question de la mobilité est centrale dans les entreprises. Le développement des réseaux haut-débit mobile permet à ces terminaux d'avoir un accès rapide et de qualité à Internet en permanence.

A ce titre, les usages en mobilité ont explosé, y compris pour les entreprises, avec de nouveaux risques de sécurité, notamment en termes de perte et de vol des terminaux.

L'utilisation d'un service de gestion des terminaux est essentiel : grâce à cet outil, il est possible de gérer à distance la destruction des données stockées sur le terminal, de le localiser, ou de le neutraliser complètement.

Authentification et SSO

Le cloud rend naturel l'utilisation de services en mobilité. Plus particulièrement, les utilisateurs peuvent retrouver à tout moment et sur n'importe quel terminal les applications dont ils ont besoin.

Si l'identification de l'utilisateur est aisée au sein de l'enceinte physique de l'entreprise, il en est autrement en situation de mobilité : le terminal d'accès peut avoir été volé, et la tentative de connexion être frauduleuse.

Ainsi, pour garantir la confiance dans l'utilisation des services Cloud, il faut avoir la certitude de l'identité de l'utilisateur.

Les différents services informatiques, Cloud ou non, demandent à l'utilisateur de s'identifier : dans le cadre de politiques de sécurité, il est régulièrement demandé à l'utilisateur d'utiliser des mots de passe complexes et différents d'un service à l'autre. Or, la réalité est toute autre : le mot de passe le plus utilisé est "123456"[18].
Avec l'essor de moyens d'attaques automatisés et puissants, l'utilisation de mots de passe complexes est critique pour garantir une sécurité des comptes utilisateurs.

En utilisant le site "https://howsecureismypassword.net/", voici un tableau comparatif du temps nécessaire pour déchiffrer un mot de passe selon sa taille.

Nombre de lettres	Nombre de chiffres	Temps nécessaire pour déchiffrer le mot de passe
0	9	3 secondes
6	2	60 secondes
0	12	4 minutes
9	3	4 ans
6	6	100 ans

Dans la dernière combinaison, en remplaçant 2 lettres par les caractères "@" et "€", le temps de déchiffrement passe à 200 ans.
Plus le mot de passe est long et complexe, plus il est efficace, au détriment de la facilité d'utilisation.

S'il est possible de générer des mots de passe forts, il est plus difficile de s'en souvenir : le piratage de TV5 Monde[19] fait suite à la diffusion accidentelle du mot de passe des serveurs de la chaîne de télévision lors d'un reportage, car inscrit sur un post-it collé au mur.
Si cette pratique n'est pas conforme aux bonnes pratiques de la sécurité, elle est pourtant malheureusement commune, et risque de s'amplifier en faisant appel aux services Cloud, avec des utilisateurs laissant à la vue de tous les mots de passe qu'ils utilisent.

[18] http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514
[19] http://www.telesatellite.com/actu/45271-des-mots-de-passe-de-tv5-monde-sur-les-images-de.html

Pour simplifier la gestion des différents comptes, et pour garantir un niveau de sécurité satisfaisant, l'utilisation d'un service de Single Sign-On (SSO) s'impose.

Ce service permet de centraliser les accès aux différents services au sein d'un seul portail, tout en garantissant l'identité de l'utilisateur grâce à un mot de passe fort pour accéder au portail, puis l'utilisation de mot de passe aléatoire pour les différents services. Ces derniers sont générés aléatoirement par la DSI, et sont volontairement cachés de l'utilisateur : l'objectif est de centraliser les connexions sur la plateforme de SSO pour permettre une gestion fine des accès.

En complément du SSO, différents outils d'authentification fortes peuvent être mis en place : en utilisant un ou plusieurs compléments au mot de passe, l'utilisateur est en capacité de prouver son identité. Si son terminal d'accès est volé, mais que les outils permettant de prouver avec certitude son identité restent en sa possession, l'accès au SI de l'entreprise reste impossible.

Détection des usages non autorisés

Aujourd'hui, un des plus importants facteurs de défiance est l'existence du Shadow IT. En effectuant la détection proactive des outils Cloud utilisés dans l'ombre, la DSI peut agir sur plusieurs plans :

- L'identification des potentielles failles de sécurité du SI.
- La compréhension des besoins non satisfaits des utilisateurs.

Le pilotage de ces usages de l'ombre pour les comprendre permet à la DSI d'agir pour mieux adresser les besoins des utilisateurs finaux, et évoluer avec eux pour le déploiement et l'utilisation sécurisée de ces outils.

Majoritairement, les utilisateurs de Shadow IT expriment leur volonté d'utiliser des outils agréés par la DSI s'ils répondent à leurs besoins : la mesure du taux d'utilisation de services non autorisés est donc un excellent indicateur de succès de la migration des applications Support vers le Cloud.

Pour cela, il faut auparavant faire émerger l'utilisation de ces usages au moyen d'outils spécialisés qui, par l'analyse du trafic réseau, mettent en lumière les accès des utilisateurs vers des services non autorisés par la DSI. Ces outils spécialisés disposent d'algorithmes de détection des usages Cloud qui viennent en complément des outils traditionnels de supervision de trafic, et qui permettent donc de mettre en oeuvre une analyse des usages à satisfaire.

Intégration des services

Enfin, pour construire un écosystème de confiance, la DSI doit aller au-delà de la sécurité, et préparer les passerelles pour faciliter la consommation des données.

Traditionnellement, les entreprises ont utilisé des ERP [20]pour produire et consommer leurs données au sein d'un même écosystème logiciel : les différents services échangent, consomment et produisent la donnée au sein d'un même référentiel partagé. Pourtant, cette démarche a montré rapidement ses limites, notamment en confrontant les utilisateurs à des systèmes lourds et peu réactifs, qui ont rapidement bridé des utilisateurs ayant besoin de plus d'agilité.

L'enjeu est de proposer un écosystème sécurisé et maîtrisé pour la consommation des données, à travers des outils d'intégration des différents services Cloud.
La poursuite d'une architecture SOA[21], avec la mise en oeuvre d'ESB[22] notamment, doit permettre aux services Cloud de pouvoir consommer la donnée sans la fragmenter, et donc de garantir la cohérence du SI de l'entreprise.
En effet, les services Cloud proposent généralement un ensemble d'APIs[23] pour préparer l'intégration avec un SI traditionnel : la mise en oeuvre d'un ESB Cloud permet d'accéder à un outil de gestion de ces APIs, et donc de sécuriser les échanges de données entre le SI traditionnel et les services Cloud.

Ce type d'outil permet ainsi de maîtriser le type de communication entre les outils, et de mettre en oeuvre des politiques spécifiques selon les utilisateurs et le type de données traitées; le choix d'un ESB Cloud est aussi une ouverture sur les futurs usages des utilisateurs, tout en conservant la maîtrise de l'utilisation des données.

B - Un marché de la confiance Cloud dense

Les différentes "briques de confiance" sont largement disponibles sur le marché, et permettent à toutes les entreprises de bénéficier de services de confiance performants à un coût raisonnable.
A ce titre, si toutes les entreprises doivent considérer ces différents services pour construire leur écosystème de confiance Cloud, elles doivent adapter le champ d'application de ces briques selon leurs besoins, leurs moyens et leurs compétences.

La liste des acteurs proposés ci-dessous n'est pas exhaustive : le marché évolue rapidement, et de nouveaux services apparaissent régulièrement. Il est ici proposé une analyse de quelques acteurs proposant des services Cloud de nature à constituer l'écosystème de confiance pour la DSI.

[20] Enterprise Ressource Planner : type de logiciel intégré pour les entreprises
[21] Service Oriented Architecture : principes d'architecture informatique pour l'intégration des services applicatifs
[22] Enterprise Service Bus : bus de communication entre les applications
[23] Application Programming Interface : un ensemble de protocole permettant l'intégration avec d'autres services.

Ces briques de confiance sont indispensables pour que la DSI puisse assurer l'utilisation des services Cloud en toute confiance : c'est par l'intermédiaire de cet ensemble de services que la DSI pourra assurer l'utilisation des applications Support en toute sécurité.

1 - Sécurité

Analyse de trafic temps réel

- **CipherCloud** Activity Monitor: Activity Monitor est un service proposé par CipherCloud permettant l'analyse en temps réel des activités des utilisateurs sur différents services SaaS. Les activités litigieuses de l'utilisateur, telles que les tentatives d'accès à des données sensibles ou l'utilisation du service en dehors des heures autorisées, sont automatiquement remontées. Le service peut être finement paramétré pour prendre en compte les spécificités de l'activité (horaires décalés par exemple). De même, Activity Monitor permet aux entreprises de respecter les obligations sectorielles auxquelles elles peuvent être soumises (PCI-DSS, données de santé,...) grâce à un ensemble de règles de sécurité respectant ces cadres juridiques. Enfin, le service étant largement interopérable avec de nombreux services SaaS, des rapports d'activités détaillés sont disponibles.
- **Zscaler** : Zscaler DLP est un service proposant l'analyse en temps réel de l'ensemble du trafic entrant et sortant vers le Cloud. Par l'intermédiaire d'un moteur de règles d'accès paramétrable et comprenant un ensemble prédéfini de règles correspondant aux différents cadres légaux auxquels les entreprises sont soumis en Europe et aux Etats-Unis. DLP propose aussi un contrôle de la bande passante utilisée, permettant d'identifier immédiatement quels sont les utilisateurs compromis. Ce service prévoit nativement la protection des utilisateurs en situation de mobilité.

Master Data Management

- **Tibco Cloud MDM** : Cloud MDM de Tibco est un service de gestion des données dans le Cloud qui peut gérer plusieurs domaines. Des templates de service sont inclus au sein du service pour accélérer le déploiement tout en respectant les obligations réglementaires. La gestion de l'accès aux données est paramétrable par utilisateur et par rôle, pour gérer finement les autorisations selon les métiers et les profils.
- **Reltio** : Cloud Master Data Management est le service proposé par Reltio pour adresser plus particulièrement la qualité de la donnée pour les CRM Cloud. Un travail poussé a été mené sur l'interface pour une utilisation simplifiée et puissante. Il s'agit d'un service reconnu comme leader sur le

marché par Gartner et Forrester. Des outils de gestion des processus et d'analytics sont inclus.

- **Semarchy** : Convergence Cloud est la réponse de Semarchy à la problématique du référentiel de données. Les politiques de gestion sont basées sur les processus et les hiérarchies, et le service propose de nombreuses possibilités d'intégration grâce à un ensemble d'APIs et de webservices. Toutes les interactions sont suivies et tracées pour garantir l'intégrité des données.

Chiffrement des données

- **SkyHigh Networks** : Le service Data Security permet la gestion et le chiffrement des données stockées dans les différents Cloud de Box, Dropbox, Google Drive, Office 365, Salesforce et ServiceNow. Si le service propose le chiffrement des données, la propriété des clés de chiffrage et de déchiffrage vous revient et n'est pas connue de SkyHigh. De plus, si vous disposez déjà de services de chiffrement, les clés utilisées pour Data Security sont compatibles avec le protocole KMIP [24]pour une gestion centralisée du chiffrement de vos données.
- **CipherCloud** : CloudsProtected est le service de chiffrement des données pour les Cloud Salesforce, ServiceNow, Office365, Sharepoint, OneDrive, Dropbox, Box, et Adobe Analytics. Les données sont chiffrées par une clé qui reste la propriété de l'entreprise, et chaque champ de données est individuellement chiffré pour garantir la confidentialité des données. En complément du chiffrement des données, le trafic est analysé pour protéger contre les attaques de malwares.
- **Netskope** : Encryption de Netskope offre la possibilité de maîtriser et de chiffrer les données des Cloud Google, Salesforce, Office 365, ServiceNow, Dropbox, Box et Egnyte. Les clés de chiffrement respectent le protocole KMIP, mais peuvent être gérées par une solution native Netskope reposant sur du matériel certifié FIPS 140-2 Level 3[25].
- **BlueCoat** : Cloud Data Security de BlueCoat permet notamment le chiffrement des données stockées dans les Cloud Public d'Oracle, Microsoft et Salesforce. Le service est évolutif, et propose nativement un environnement pour paramétrer le chiffrement vers de nouveaux fournisseurs Cloud. Les réglementations supportées nativement sont nombreuses mais couvrent principalement les normes américaines.

Masquage de données

- **Camouflage** : CX-MaaS est le service en ligne de masquage des données proposé par Camouflage. Ce service à la demande inclut CX-Discover et

[24] Key Management Interoperability Tool : protocole de communication pour les clés de chiffrement
[25] Norme gouvernementale américaine de certification des composants de chiffrement

CX-Mask, qui permettent d'identifier les données sensibles du SI, puis traitées par CX-Mask pour l'utilisation à des fins de tests ou de prototypage.

- **CloudMask** : CloudMask est un service spécialisé pour le masquage des données sur Gmail, Google Drive et Clio, avec une expertise forte dans les industries de l'Education, la Justice, la Santé et le Secteur Public.

Firewall Cloud

- **Qualys** : Acteur spécialisé des PME, Qualys propose un service Cloud de filtrage du trafic. Qualys revendique l'analyse de plus de 3 milliards d'adresses IP par an, une disponibilité de 99.95%, et une fiabilité de l'analyse supérieure à 99.99966% selon les critères Six Sigma.
- **Virtela** : Virtela est un acteur Cloud proposant un service couvrant l'ensemble des services de sécurité. Son échelle mondiale, et la présence d'une équipe de sécurité disponible 24/7 sont des atouts pour les entreprises présentes partout dans le monde.

Gestion de terminaux

- **Airwatch** : AirWatch est la solution leader du marché de la gestion de terminaux. Compatible avec l'ensemble des systèmes d'exploitation du marché fixe et mobile, AirWatch facilite la gestion des flottes de terminaux, et permet à l'entreprise de mettre en oeuvre de nouvelles politiques de terminaux (comme le Bring-Your-Own-Device[26]). AirWatch propose en complément des applications sécurisées pour les utilisateurs (stockage hors ligne, navigateur internet,...).
- **MobileIron** : MobileIron supporte les trois plus grands systèmes d'exploitation du marché (Windows, Android, iOS). Son écosystème complet permet de gérer les terminaux, les applications mobiles de l'entreprise et de sécuriser les données mobiles.
- **Microsoft** : InTune est un service Cloud de Microsoft pour gérer les terminaux Apple, Android et Windows. Intégré dans le service Enterprise Mobility de l'éditeur, Intune permet aussi la gestion des applications et de l'intégration avec les applications mobiles de l'éditeur.

2 - Authentification et SSO

SSO

- **Ping Identity** : PingOne Cloud est une des solutions de référence du marché du SSO, et inclut nativement la possibilité de centraliser les accès pour plus

[26] L'utilisateur choisit son terminal, et l'entreprise procède à son intégration dans le SI.

de 1.500 services Cloud. Le service comprend aussi une plateforme complète de gestion des identités et un service d'authentification forte.

- **CloudAccess** : Le service Identity Management de CloudAccess a pour spécificité d'automatiser l'ajustement des profils d'accès des utilisateurs à travers tous les services utilisés par l'entreprise. Le service inclut aussi la gestion de terminaux.
- **OneLogin** : OneLogin est une autre solution de référence du marché, et gère l'accès à plus de 4.000 services nativement. Disponible sur l'ensemble des terminaux, OneLogin propose aussi un service d'authentification forte.
- **Centrify** : Centrify est reconnu comme leader par Gartner dans la fourniture de service SSO. En intégrant nativement la gestion des terminaux et l'authentification forte, Centrify propose un service complet pour la gestion de l'authentification des utilisateurs dans le Cloud.
- **Okta** : Okta centralise l'accès à plus de 5.000 services Cloud. En complément d'un service prêt à l'emploi, Okta propose une plateforme aux développeurs pour compléter les fonctionnalités du service. Sur les 12 derniers mois, Okta a assuré une disponibilité à 99.98% de son service.

3 - Détection des usages non autorisés

- **SkyHigh Network**: SkyHigh for Shadow IT est un service de détection et de pilotage des usages Cloud pratiqués par les utilisateurs. Grâce à sa base de données de 20.000 usages Cloud, SkyHigh qualifie le risque de l'utilisation sur une échelle de 1 à 10. La surveillance en continue s'améliore en permanence grâce à ses 30 millions d'utilisateurs qui améliorent la pertinence du service.
- **CipherCloud** : CloudDiscovery de CipherCloud permet d'exposer au grand jour les usages de l'ombre. Les risques sont identifiés au sein d'un tableau de bord, et bénéficient des analyses d'organismes tels que Forrester ou la Cloud Security Alliance pour pouvoir remédier à ces risques de façon efficace.

4 - Intégration des services

ESB Cloud

- **Zapier** : Zapier est un service intuitif de mise en relation de services Cloud. Avec une interface par glisser-déposer, et un catalogue fourni de liens entre 700 applications, il s'agit d'un service simple et efficace.
- **Mulesoft** : La plateforme Mulesoft permet une intégration poussée et personnalisée des services Cloud. Les intégrations avec Salesforce, Office 365 et ServiceNow sont prévues nativement.

- **Apigee** : Apigee propose un service par secteur d'activité, en prévoyant les évolutions liées à l'Internet des Objets et la monétisation des APIs. Ce service inclut aussi une plateforme de suivi de l'utilisation des différentes APIs.
- **Mashery** : Mashery permet la gestion complète du cycle de vie de l'API, depuis sa création jusqu'à son utilisation. Couvrant les besoins de l'internet des objets, Mashery comprend aussi la mise à disposition des données vers les terminaux mobiles.

5 - Gagner du temps avec les CASB

Le terme CASB désigne les "Cloud Access Security Brokers". Le cabinet d'analystes Gartner définit les CASB comme des points d'accès physiques ou virtuels proposant plusieurs services de sécurisation d'accès aux services Cloud.

Le cabinet estime qu'en 2020, 85% des grandes entreprises utiliseront ce type de service pour sécuriser leurs usages Cloud; en 2015, ce marché représentait un volume supérieur à $185m.

Le choix d'un CASB n'est pas anodin : il s'agit d'un véritable accélérateur dans la consommation des services Cloud qui apporte la confiance technique nécessaire dans l'utilisation d'outils dont l'exploitation n'est plus assurée par la DSI.
De même, le choix du CASB doit répondre à la réalité des contraintes de l'entreprise : le profil de l'entreprise conditionne le choix entre une solution sur mesure et une solution sur étagère centralisée proposée par un CASB.

En complément de certains acteurs identifiés ci-dessus, tels que **SkyHigh Networks**, **BlueCoat**, **CipherCloud, Netskope** et **Zscaler**, on peut distinguer les acteurs suivants :

- **Imperva** : Imperva est identifié par Gartner comme le leader des WAF (Web Applications Firewall). Son offre de service Cloud est orientée sur la protection des réseaux et des accès : SkyFence est un service permettant notamment de découvrir les usages Cloud non autorisés, de mettre en place des politiques de sécurité Cloud pour garantir la conformité avec les cadres réglementaires, et d'activer ces politiques à travers l'ensemble de leurs services Cloud de façon automatisée.
- **Bitglass** : Bitglass se distingue par une protection temps-réel des usages Cloud, et par une offre de services complète. Depuis le SSO des utilisateurs jusqu'au chiffrement des données, en prenant en charge la sécurité du réseau et la détection des services non autorisés, Bitglass permet un déploiement rapide d'un écosystème de confiance Cloud.

III - Construire et valider l'écosystème de confiance

La mise en oeuvre d'un écosystème de confiance Cloud ne s'improvise pas, et doit faire l'objet d'une approche structurée dans sa construction.

Les besoins techniques à satisfaire doivent répondre à des impératifs liés aux utilisateurs finaux : tous les utilisateurs ne sont pas égaux.
Selon leur profil, c'est à dire le métier exercé et leur appétence pour les outils informatiques, les mesures de confiance à déployer sont radicalement différentes.

Une fois l'écosystème construit, il est primordial de le confronter à la réalité par une expérimentation reflétant les conditions réelles d'utilisation, avant de procéder à un déploiement généralisé.

A - Construction de la matrice de décision

Chaque entreprise doit se livrer à une analyse précise de ses besoins en matière de sécurité et de confidentialité : une entreprise disposant de plusieurs sites à travers le monde et oeuvrant dans une industrie hautement innovante ne nécessite pas les mêmes mesures qu'une PME qui a localisé sa production en Bourgogne et qui sert une clientèle locale.
Cette analyse doit être menée au cas par cas, et est spécifique à chaque entreprise, et à chaque activité de l'entreprise considérée.

L'audit préalable sur les mesures de sécurité en place et à déployer pour sécuriser les usages Cloud est indispensable, et doit faire émerger les niveaux de service exigés pour chacune des briques.
Ces mesures de sécurité à déployer permettront aussi d'identifier si le recours à un CASB est crédible.

Chacune des briques de confiance répond à un problème clairement identifié pour l'entreprise :

- La sécurité est un point critique pour les entreprises, tant d'un point de vue respect de la confidentialité des données que résilience de l'activité.. Ainsi, si les données doivent être identifiées et classifiées selon leur niveau de criticité (les données liées à la Recherche et au Développement n'ont pas la même valeur que les données liées au Marketing), il est essentiel d'assurer la continuité de l'activité de l'entreprise.
- L'authentification doit être considéré au cas par cas selon la typologie des populations utilisatrices : les utilisateurs nomades, comme les forces de vente, sont amenés à utiliser les services à l'extérieur, et sont donc des proies

pour des personnes mal intentionnées. A l'inverse, un utilisateur n'utilisant jamais les applications de l'entreprise en dehors de son lieu de travail ne présente pas le même risque.

- La sécurité du réseau est un enjeu qui dépasse les utilisateurs : la DSI doit considérer quel est le niveau à proposer en matière de performance réseau et de convivialité des usages en mobilité. Il est fortement probable que l'entreprise dispose déjà d'infrastructures de sécurité; l'enjeu est ici de comprendre quel niveau de criticité est associé à l'utilisation des services Cloud, et de quel façon il faut assurer la protection de ces accès.
- L'analyse des usages non autorisés doit permettre à la DSI d'identifier quels usages de l'ombre doivent être adressés, et travailler avec les utilisateurs pour satisfaire ces besoins.
- L'intégration des services représente un enjeu fort : s'il ne s'agit pas en soi d'une brique technique de sécurité, l'intégration des services permet de valider la consommation des données du SI existant, tout en limitant la fragmentation qui pourrait résulter de l'utilisation et de la génération de données, externes au SI, mais par la suite réintégrées au sein de celui-ci. Le besoin d'intégration varie selon le secteur d'activité, la taille de l'entreprise, mais aussi son existant SI : le besoin d'intégration peut être extrêmement limité si le référentiel de données existant est faible; mais il est nécessaire de prévoir la construction de données cohérentes.

Enfin, le critère final de décision devra être le degré de maîtrise sur son écosystème que la DSI souhaite opérer. Le choix d'un écosystème sur mesure, où chaque solution est sélectionnée individuellement et orchestrée au sein du SI de façon indépendante, est possible, le coût et le temps de déploiement de ce type d'écosystème le réserve à des entreprises de niche, disposant d'un capital financier important à consacrer à ce projet, ainsi que d'expertises importantes dans le domaine de la sécurité informatique.

Ces expertises sont rares; il peut être plus pertinent pour la DSI de s'orienter vers un CASB capable de l'assister rapidement et efficacement dans le déploiement d'un écosystème de confiance qui lui permettra de basculer au plus vite vers les usages Cloud pour les applications Support.

Cette matrice de décision doit être employée au niveau de chaque métier, et prendre en compte les spécificités des différentes activités de l'entreprise, y compris la localisation des différentes équipes.

En effet, les régimes légaux varient grandement d'un pays à un autre, et certaines briques peuvent s'avérer nécessaires pour un type d'activité, mais accessoire pour d'autres : par exemple, le masquage de données est nécessaire pour des équipes

manipulant des données personnelles, mais se révèle inutile pour les équipes en charge du contrôle de gestion projet.

1 - Méthodologie

Pour classer les exigences de service de chacune des briques de confiance, on peut utiliser l'échelle suivante :

- **Non nécessaire**: ce critère fait référence à un besoin qui a été analysé mais déjà adressé avec les solutions existantes déjà en place et satisfaisant les critères de confidentialité auxquels l'entreprise est soumise.
- **Standard** : le niveau standard traduit une exigence qui a été analysée, mais qui ne justifie pas le déploiement d'un moyen de sécurisation particulier de par la nature des données manipulées par les utilisateurs et le profil de ces derniers.
- **Intermédiaire** : le niveau intermédiaire traduit qu'une maîtrise de cette brique de l'écosystème est nécessaire. Par exemple :
  - Les utilisateurs sont nomades.
  - Le secteur d'activité est fortement concurrentiel, et la débauche de personnel est une pratique courante.
  - Les utilisateurs sont répartis sur plusieurs sites géographiques.
- **Critique** : le niveau critique demande un contrôle très fin de cette brique de l'écosystème en raison d'impératifs légaux ou stratégiques. L'activité de la population utilisatrice ciblée est considérée comme critique pour l'entreprise, et doit donc être strictement encadrée. On peut par exemple considérer les cas suivants comme nécessitant un degré critique :
  - Les utilisateurs manipulent des données de patients.
  - L'activité de l'entreprise repose majoritairement sur des activités de Recherche et Développement dans un secteur ultra-concurrentiel.
  - Les informations personnelles des clients et des employés sont manipulées régulièrement par certains employés.
  - L'activité de l'entreprise est strictement encadré, et fait l'objet de réglementations spécifiques.
  - L'entreprise est un OIV [27].

Pour établir cette exigence de service et construire sa matrice de décision, il est nécessaire d'ajouter les éléments suivants :

- Typologie des utilisateurs cibles
- Criticité de l'activité des utilisateurs cibles

[27] Opérateur d'Importance Vitale

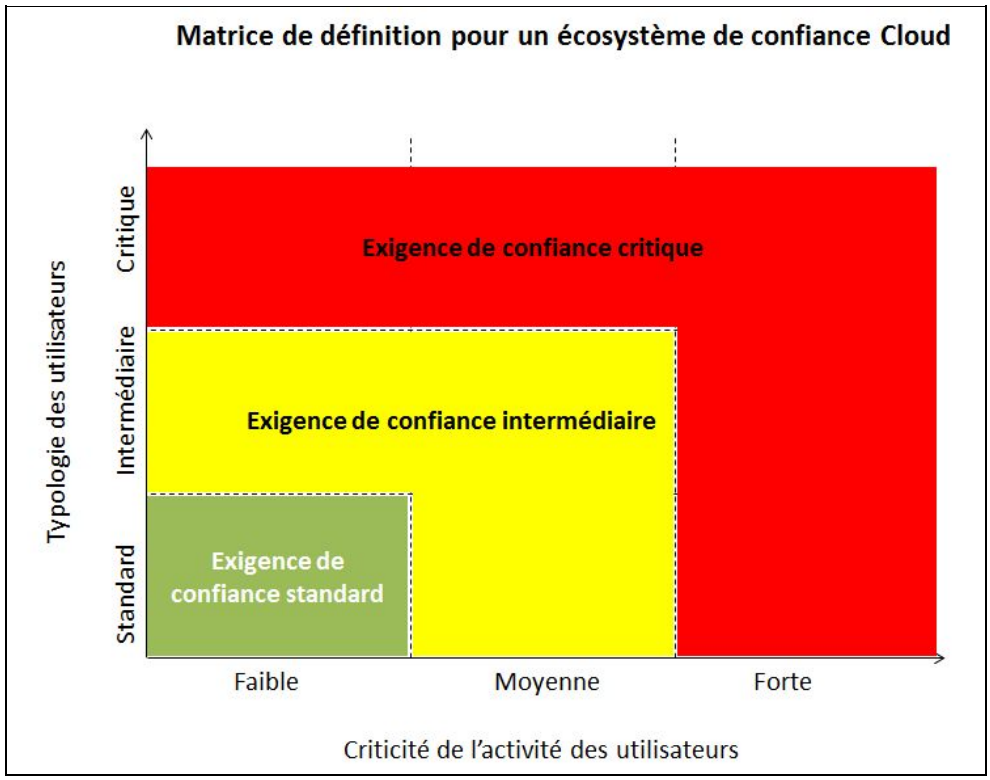
La typologie des utilisateurs peut être décomposée en 3 catégories. Les caractérisations sont données à titre indicatif :

- **Standard** : les utilisateurs “standards” sont par exemple les utilisateurs sédentaires, n’accédant jamais au SI de l’entreprise en situation de mobilité ou en dehors des sites de l’entreprise.
- **Intermédiaire** : ces utilisateurs ont une utilisation ponctuelle en dehors de l’entreprise du SI de l’entreprise, et disposent d’un smartphone fourni par l’entreprise pour l’accès mobile.
- **Critique** : ces utilisateurs ont été pionniers dans l’utilisation d’outils informatique de l’ombre,et accèdent régulièrement au SI de l’entreprise en dehors des horaires classiques.

Pour établir la criticité de l’activité des utilisateurs, il faut distinguer les 3 échelons suivants :

- **Faible** : il s’agit d’une activité n’impliquant à aucun moment le traitement et l’échange de données sensibles de l’entreprise.
- **Moyenne** : l’activité demande, de façon très ponctuelle et selon le profil des utilisateurs, le traitement de données sensibles.
- **Forte**: Toute activité relative à des opérations stratégiques perçues comme vitale pour l’activité de l’entreprise : Recherche et Développement, Secret Défense, Données de santé, Données personnelles,...

Pour faciliter la définition du niveau de criticité des données manipulées, une analyse des données selon le degré de Disponibilité, Intégrité, Confidentialité et Traçabilité peut être menée en travaillant avec les métiers et le RSSI pour établir les exigences liées à chacun des éléments.



Grâce à cette matrice, la DSI est capable de positionner précisément quel type d'exigence déployer selon le type d'utilisateur et d'activité.

En positionnant l'exigence nécessaire face aux différentes briques constitutives de l'écosystème de confiance, la DSI est capable de construire un "cahier des charges" de l'écosystème à construire pour sécuriser les usages Cloud.

Ce cahier des charges doit établir précisément les caractéristiques techniques minimum que l'écosystème de confiance doit présenter afin d'accomplir sa mission, et ce en coopération avec le Responsable Sécurité du Système d'Information.

Pour établir les critères techniques de sélection des briques de confiance Cloud, il est possible d'établir un tableau de critères selon les différents niveaux d'exigences, en coordination avec les experts en sécurité SI de l'entreprise.
Le cas échéant, le tableau des critères peut être établi en accord avec l'expertise d'un cabinet de conseil spécialisé, qui pourra être chargé de la réalisation et de la mise en oeuvre de l'écosystème de sécurité.

2 - Cas pratique

Pour illustrer l'utilisation de la matrice, et de l'écosystème de confiance, prenons le cas suivant.

Une entreprise industrielle familiale en province, leader sur son marché, disposant d'une ligne de production et d'un service de Recherche et Développement, souhaite favoriser l'utilisation des services Cloud : en effet, les outils composant son Système d'Information sont vieillissants, et ne répondent plus de manière satisfaisante aux besoins de l'activité. De plus, le département SI souhaite se concentrer sur ses activités à forte valeur ajoutée plutôt que sur le maintien de solutions obsolètes et coûteuses.

Plusieurs populations sont à distinguer au sein de l'entreprise :

- **La direction de l'entreprise**, et plus particulièrement le Directeur, qui a repris l'entreprise suite à la retraite de son père; habitué des services de stockage en ligne dans son ancien métier, il est resté ancré sur ses habitudes.
- Le personnel historique de l'entreprise, principalement pour les services **Back-office**, qui a subi la révolution informatique, et qui tente de s'adapter aux nouveaux outils.
- **Les ingénieurs du service de Recherche et Développement**, dont les terminaux ont un accès restreint vers l'extérieur, et qui disposent de moyens de sécurité avancés, comme par exemple le chiffrement systématique des données.
- Enfin, **les commerciaux** de l'entreprise, itinérants par nature et qui disposent de terminaux mobiles, aussi bien téléphones qu'ordinateurs. Utilisant aussi bien les véhicules de l'entreprise que les transports en commun, un historique fort existe de terminaux perdus.

Considérant la forte disparité des usages, et des attentes des utilisateurs, il faut adapter l'écosystème à la typologie de l'utilisation et de son contexte : en prenant en compte les typologies d'utilisation des outils informatiques, ainsi que les profils des utilisateurs, il est nécessaire d'accorder l'exigence de confiance grâce à la présence de l'écosystème.

Pour établir la grille d'exigences, reprenons les populations identifiées auparavant.
Pour chacune des briques de confiance, il est nécessaire d'accorder le niveau d'exigence à la typologie d'utilisateur et à la criticité de son activité; de même, il faut identifier quelles sont les briques de confiance à activer, et celles qui ne présentent pas d'intérêt.

En effet, la mise en oeuvre d'un écosystème de confiance permet tout autant de faciliter l'utilisation des services Cloud que d'apporter le niveau adéquat d'encadrement des services en terme d'utilisation et de sécurité.

Pour cela, il faut donc clairement identifier la typologie des utilisateurs qui seront concernés par cet écosystème.

Cette classification des utilisateurs doit se faire selon des critères relatifs à leurs cas d'usage de l'informatique, leur activité, mais aussi leur exposition aux risques physiques et informatiques.

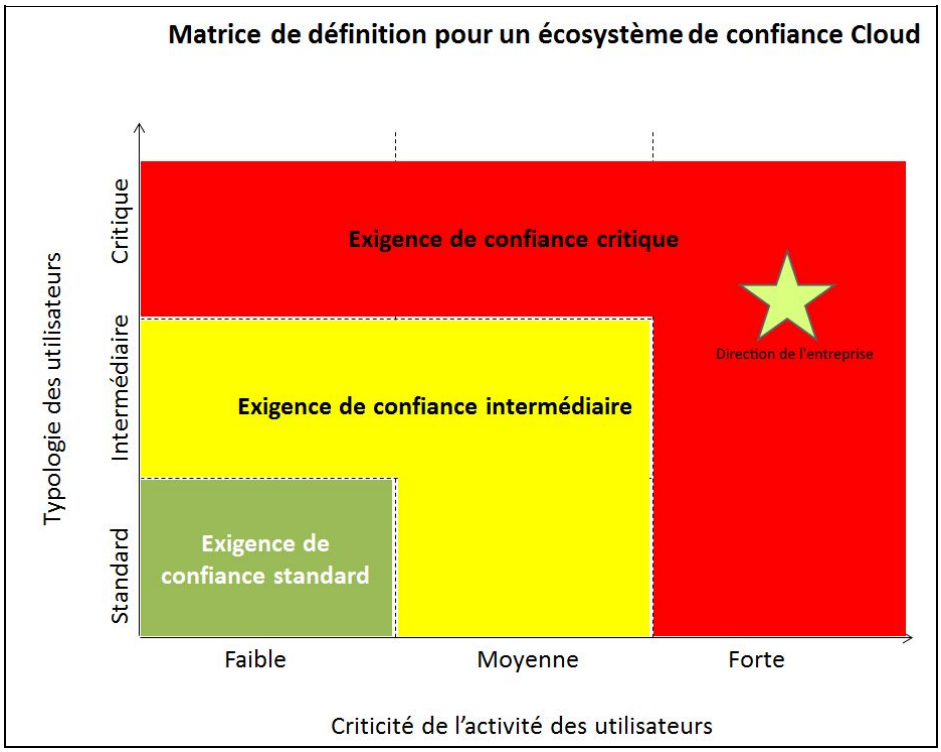
Ainsi, il faut **adapter la grille** des critères à l'activité de l'entreprise; pour autant, on peut dégager des critères standards qui devront être abordés de façon incontournables :

- L'utilisation en **mobilité** : la population étudiée utilise-t-elle de façon quotidienne l'informatique en dehors des locaux de l'entreprise? Accède-t-elle à la messagerie de l'entreprise par l'intermédiaire de son smartphone?
- S'agit-il d'une population utilisateur qui a fréquemment recours au support informatique? Cette population présente-elle des antécédents de demandes au support suite à une infection d'un virus informatique?
- Existe-il des **antécédents de perte et/ou de vol** des terminaux de l'entreprise?
- Plus globalement, les données utilisées par cette population d'utilisateurs sont-elles sensibles? Est-il aisé d'identifier les cas d'utilisation anormale des outils informatiques?
- L'équipe informatique de l'entreprise est-elle structurée de façon à pouvoir assurer un soutien immédiat au plus proche des utilisateurs?

Dans notre exemple, prenons le cas de la **direction** :

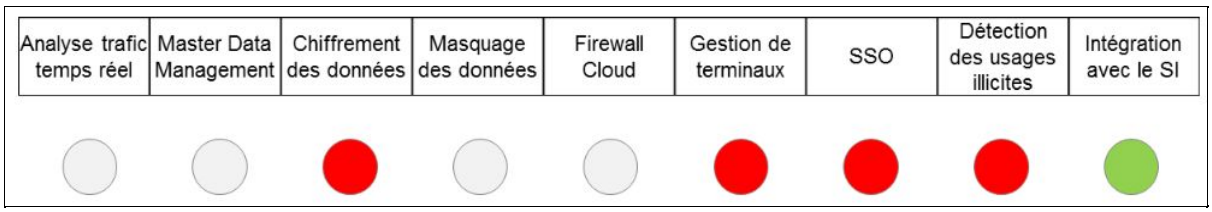
- Le dirigeant est un adepte familiarisé des outils Cloud : ses usages incluent le stockage en ligne par des services comme Dropbox, et le partage des documents stockés sur ces services aussi bien vers le personnel de l'entreprise que vers des partenaires.
- De par la nature du poste, il est régulièrement en déplacement : en effet, le site est en province, mais ses partenaires ne sont pas dans les environs. Il accède donc régulièrement aux données de l'entreprise depuis l'extérieur, et ce avec son smartphone et son ordinateur portable.
- Le personnel rattaché à la direction d'une entreprise incarne une cible de choix pour les attaquants : il s'agit de postes à haute visibilité, avec un accès étendu aux ressources informatiques de l'entreprise. Ainsi, compromettre ce type de compte est généralement la garantie d'un accès facilité à l'ensemble du système d'information de l'entreprise.

Par cette analyse, nous pouvons déjà positionner le profil de dirigeant de la façon suivante sur la matrice de définition de l'écosystème de confiance :



En examinant de façon plus fine les besoins et les cas d'usage liés à la direction de l'entreprise, il est possible d'établir une grille d'exigence pour l'écosystème de confiance Cloud à construire.

Ainsi, pour notre cas pratique, on retrouve les exigences suivantes pour l'écosystème de confiance Cloud relatif à la direction de l'entreprise :



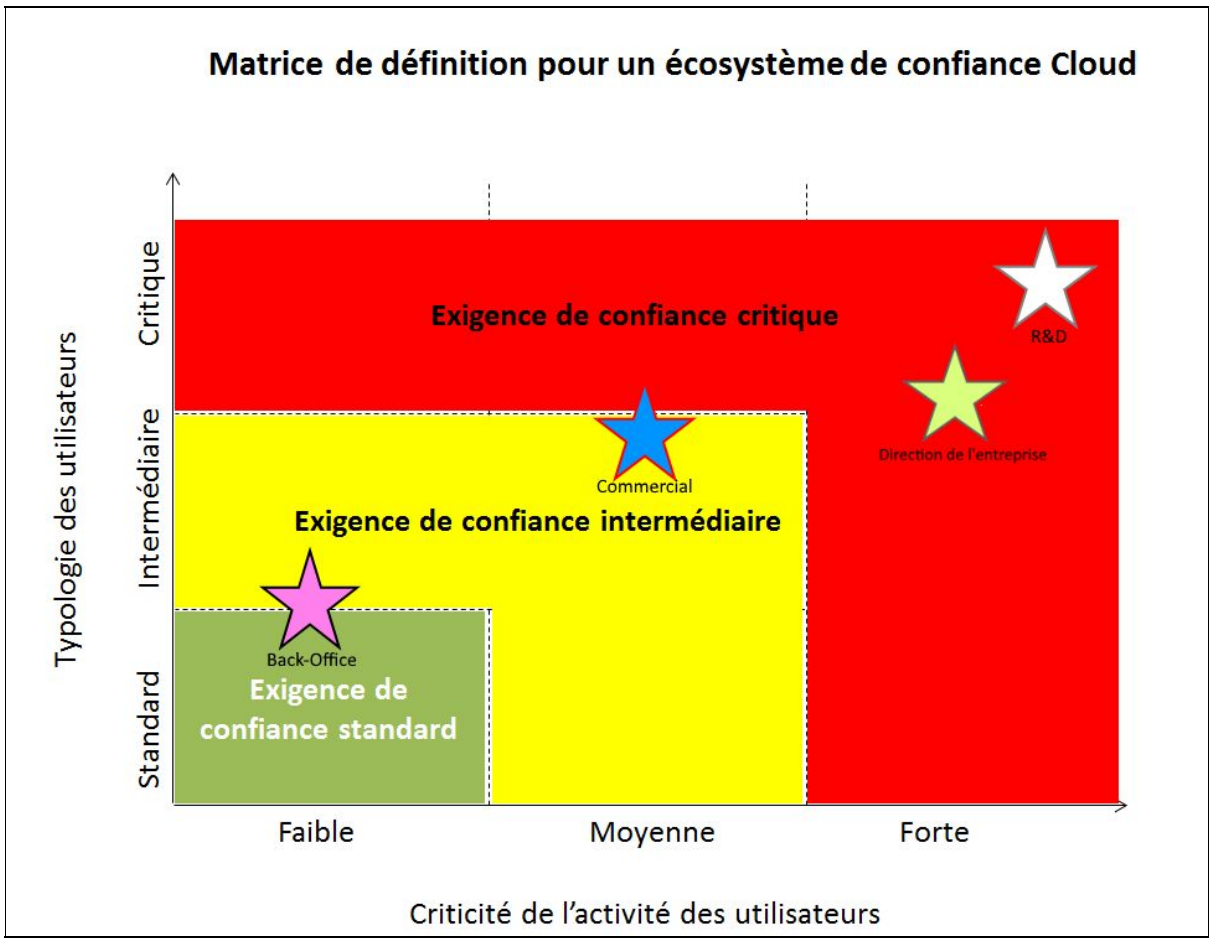
Ainsi, il n'est pas nécessaire de déployer l'ensemble des briques de confiance pour répondre aux besoins de confiance dans les outils Cloud pour ce cas d'usage précis.
Les points essentiels sont les suivants :

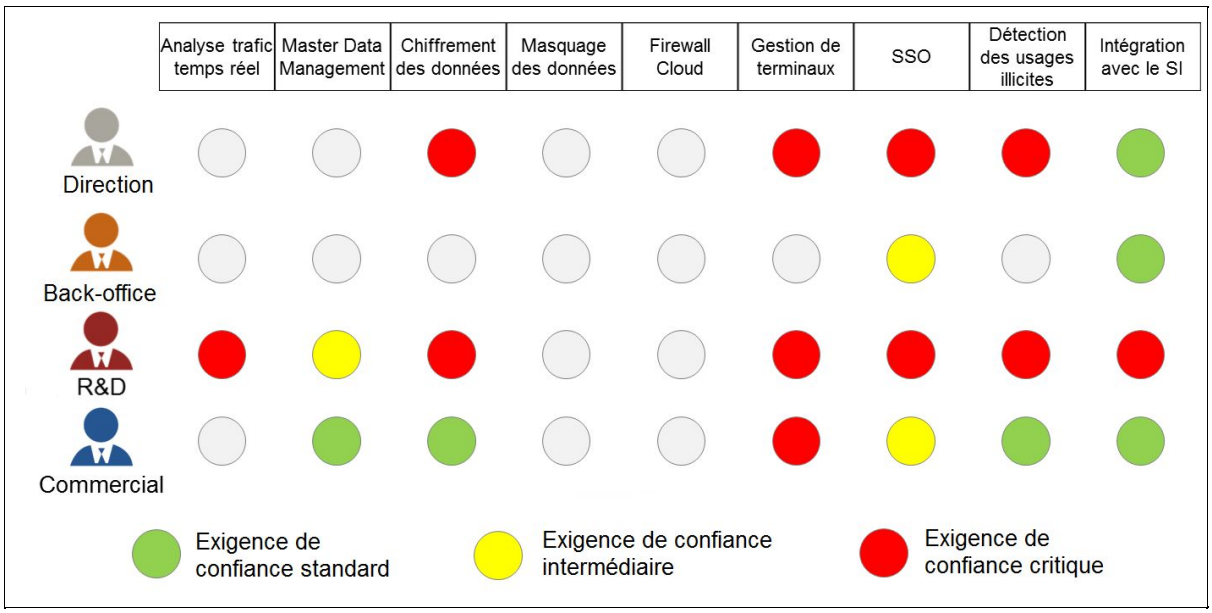
- Pour se prémunir de l'accès aux données sensibles, il convient de chiffrer les données d'une façon forte.
- La possibilité de gérer le terminal de l'utilisateur est clé : il s'agit d'une population itinérante, qui peut faire l'objet de tentatives physiques d'accès aux données : le vol d'un des terminaux des utilisateurs est une possibilité réelle.
- De même, la mise en place d'un SSO s'impose : tant pour des raisons de commodité d'utilisation des outils Cloud que pour faciliter la gestion des accès

aux différents services (et donc restreindre ces derniers en cas de compromission), cet outil doit s'imposer comme un vecteur facilitateur de recours au Cloud.

- La possibilité de détecter des usages non autorisés est aussi un cas essentiel : dans notre exemple, cela permettra d'encadrer les usages introduits par le dirigeant familier des outils Cloud au sein de l'écosystème; cela permettra aussi de détecter une possible tentative d'exfiltration des données.
- Enfin, la direction de l'entreprise ne peut pas bénéficier d'un système d'information parallèle dédié : cela serait contre productif compte tenu de la taille de l'entreprise et des gains potentiels. En conséquence, l'anticipation de ce besoin particulier est essentielle, et doit permettre de participer à la cohérence des données du système d'information de l'entreprise.

En répétant l'exercice pour l'ensemble des populations identifiées dans l'entreprise, l'on obtient les matrices suivantes :





Matrice d'exigences de confiance

Ainsi, les exigences de confiance les plus fortes portent sur les populations critiques de l'entreprise, à savoir la direction et la Recherche & Développement : que ce soit en termes de briques activées ou du niveau d'exigence à délivrer, ces deux populations doivent être plus fermement encadrées dans leurs usages de services Cloud que les autres populations de l'entreprise.

Certains services particuliers, comme le Master Data Management, ne doivent pas être généralisés à tous les utilisateurs : l'enjeu de ce type de service est de garantir la cohérence du référentiel de données, mais aussi de limiter les accès par des populations non autorisations potentiellement plus vulnérables aux attaques informatiques.

Par ce cas pratique et l'utilisation de la matrice présentée auparavant, l'utilisation d'un écosystème de confiance permet donc d'adapter finement les mesures techniques permettant d'accompagner l'utilisation des services Cloud : l'enjeu de l'écosystème de confiance n'est pas de déterminer une seule typologie de service, avec un unique degré d'encadrement qui doit prévaloir pour l'ensemble des utilisateurs.
Cette démarche serait contre-productive, et surtout coûteuse : le recours à un écosystème de confiance doit permettre d'adapter tout autant l'encadrement du service que le service en lui-même : l'écosystème accomplit le rôle de cockpit de pilotage des ressources Cloud à travers de multiples fournisseurs, en offrant le bon service à la bonne population, au sein d'un écosystème sain pour l'activité de l'entreprise.

La détermination technique de l'exigence de confiance doit être faite par le DSI, accompagné le responsable de la Sécurité Informatique, et doit être mené au cas par cas : il est essentiel de distinguer une gradation dans les exigences, afin de pouvoir mettre en oeuvre la confiance adéquate au vu du service, de l'utilisateur, et du budget alloué.

B - Validation

L'écosystème de confiance établi et mis en oeuvre, il est primordial de procéder à sa validation pour procéder ensuite à son déploiement généralisé.

1 - Prérequis

Pour autant, la DSI doit avoir anticipé cette procédure en ayant procédé à certaines étapes préalables obligatoires :

- **Un audit et une classification des données** doit avoir été menée : d'après une étude du Bureau Veritas de 2015, en France, 57% des données d'une entreprise ne sont pas identifiées, 21% des données identifiées sont des doublons de données existantes et seules 22% des données sont pertinentes [28]. Or, toutes les données ne sont pas égales : les données personnelles ont une valeur plus importante, et leur utilisation est encadrée juridiquement. De plus, cette classification permet aussi de faciliter le travail préparatoire de construction de l'écosystème de confiance, en identifiant clairement quels sont les types de données que les utilisateurs manipulent, et ce par profil.
- L'écosystème de confiance prévoit l'intégration des applications SaaS avec le reste du SI : il faut donc **veiller à ce que les services SaaS disposent d'APIs**.
- L'utilisation d'un écosystème de confiance Cloud et de services SaaS requiert une **revue du paramétrage des moyens de sécurité déjà en place** au sein de l'entreprise (Firewall notamment).

2 - Expérimentation

Une fois ce travail préparatoire effectué, et l'écosystème Cloud à tester prêt, il est essentiel de procéder à une phase de prototypage par l'intermédiaire d'un Proof of Concept.

L'objectif de cette phase est de tester et de confronter la validité des choix techniques effectués lors de la construction de cet écosystème de confiance.

Cette phase doit inclure les points suivants :

- La **définition précise des indicateurs** validant le fonctionnement de l'écosystème de confiance.

28 http://images.info.veritas.com/Web/Veritas/%7B364a7ca5-e05c-4fce-971b-88e18c62eafb%7D_45145_EMEA_Veritas_Strike_Report_Gulf.pdf

- Les **tests par des utilisateurs finaux**, idéalement utilisateurs de Shadow IT, pour valider la pertinence de l'usage offert par l'écosystème de confiance.
- Le **suivi de la qualité de service** offerte par les différents fournisseurs par l'intermédiaire de robots simulant un utilisateur.
- Des **tests d'intrusion, complétés d'un programme de bug bounty**[29] au sein de l'écosystème de confiance Cloud.
- Une phase de **recueil de la satisfaction des utilisateurs finaux** par rapport à l'expérience offerte par l'écosystème de confiance.

La phase d'expérimentation doit être l'occasion de valider les différentes compétences requises pour l'opération technique de l'écosystème, ainsi que la confrontation entre les exigences identifiées par la DSI et le RSSI et la réalité des utilisateurs de tests.

Le recours aux utilisateurs ayant un recours régulier au Shadow IT est primordial : l'un des objectifs poursuivis par le déploiement de l'écosystème de confiance est la généralisation des services SaaS dans un cadre autorisé par la DSI.
Les retours de ces utilisateurs mettront en avant les avantages de cet écosystème par rapport au Shadow IT, limitant ainsi l'utilisation de ces outils non sanctionnés par l'entreprise.

3 - Déploiement

Enfin, ce prototype doit servir d'initiateur à un déploiement généralisé à l'ensemble des équipes de l'entreprise : pour cette dernière phase, si la DSI est techniquement apte à assurer seule ce déploiement, le projet d'écosystème de confiance Cloud inclut des aspects relatifs à la conduite du changement qui peuvent être portés par des partenaires.
La mise en oeuvre de nouveaux outils, le changement d'approche pour la gestion du SI et des applications, mais aussi la communication et la formation des utilisateurs implique un travail de fond pour favoriser l'émergence d'un fonctionnement fluide de l'entreprise vers le Cloud.

Le recours à une expertise externe est une opportunité de capitaliser sur des expériences d'accompagnement au changement et de sensibilisation des utilisateurs sur les bonnes pratiques offertes par les services SaaS.
En effet, le recours généralisé au SaaS pour les applications Support doit permettre à la DSI de se concentrer sur ses missions principales liées à l'Infrastructure et aux applications coeur de métier : la validation de la pertinence de l'écosystème de confiance Cloud par les utilisateurs finaux est clé dans l'atteinte de cet objectif.

[29] Bug bounty : Programme ouvert au public pour la découverte de bugs ou failles de sécurité. Les participants qui ont trouvé une bug ou une faille sont récompensés.

Conclusion

Le Cloud s'impose de plus en plus comme un moyen incontournable de moderniser les systèmes d'information des entreprises, et cette tendance ne fait que s'amplifier : à ce titre, refuser l'utilisation des outils Cloud revient pour une DSI à s'enfermer dans une impasse qui la condamne à terme à l'impuissance.

Cette attitude de défiance vis à vis de l'informatique en nuage ne peut plus perdurer. Les entreprises ont accès à une gamme complète de services pour générer la confiance qui jusque là pouvait leur manquer.

La DSI doit prendre sa place, et être le premier support de ces usages Cloud.

La DSI dispose de tous les outils pour faciliter l'adoption des usages Cloud, et ce pour son propre bénéfice : la DSI doit se concentrer sur ses missions à forte valeur ajoutée pour conserver l'entièreté de sa pertinence au sein de l'entreprise.

Cette pertinence passe par un recentrage sur la gestion et le développement des aspects Infrastructure et Coeur de métier du SI, en déléguant la fourniture des applications Support aux fournisseurs Cloud.

Le déploiement d'un écosystème de confiance, sécurisant les transactions entre le SI de l'entreprise et les services Cloud permet de faire émerger cette nouvelle réalité

Cet écosystème doit faire passer un message fort : le Cloud est une réponse crédible aux enjeux de l'entreprise, et la DSI est un acteur puissant pour permettre aux métiers d'accéder à des usages innovants, pertinents et à forte valeur ajoutée pour l'entreprise.

La menace des usages fantômes s'efface devant un écosystème qui promeut l'ouverture vers des services Cloud, et qui neutralise donc l'attrait de ces services non autorisés et vecteurs de risques à tous les échelons de l'entreprise.

Cette neutralisation de l'informatique de l'ombre, liée à l'adoption des services Cloud, est une opportunité à saisir pour la DSI. Au delà des aspects techniques et informatiques, l'évolution des usages est une porte ouverte à une discussion de fond avec les métiers sur l'avenir à construire pour les usages de l'entreprise.

La construction d'une gouvernance des usages Cloud mixte, mêlant l'expertise technique de la DSI et la vision des usages des métiers, permet de faire émerger un terreau d'échanges pour générer l'innovation par les nouveaux usages.

Cette gouvernance mixte entre la DSI et les métiers doit permettre de générer de nouveaux processus pour la consommation des services Cloud. Ces services sont soumis à des contrats particuliers, avec des législations particulières; de même, le

mode de tarification à l'usage et au mois peut entraîner des confusions auprès de décideurs habitués à des schémas directeurs sur 3 à 5 ans.

Il est donc indispensable de solliciter les équipes juridiques et achats en plus des équipes métiers : l'équipe juridique apporte son expertise légale pour comprendre les risques contractuels, et l'expertise des acheteurs doit aboutir sur un processus d'achat et de négociation efficace et en ligne avec les bonnes pratiques de l'entreprise.

La construction technique de l'écosystème de confiance Cloud ne doit cependant pas faire oublier les autres aspects à prendre en compte. Si la DSI est capable de déployer un environnement lui permettant de consommer en toute confiance des services Cloud, certaines industries sont soumises à des contraintes fortes qui les conduisent à rechercher des certifications particulières.

Cet écosystème de certifications est en construction : l'ANSSI[30] va proposer incessamment une certification visant à assurer les clients d'une garantie de sécurité et de confidentialité des données; l'association Cloud Confidence élabore un référentiel de certifications visant à rassurer les entreprises sur les modalités contractuelles, la localisation des données, et la sécurité des donnée; enfin, la Cloud Security Alliance propose déjà des certifications pour les fournisseurs et les entreprises respectant un ensemble de bonnes pratiques liées à la sécurité informatique dans le Cloud, mais elle manque de rayonnement en France pour bénéficier d'une réelle portée.

De même, la DSI a vocation à être le bras armé technique de la consommation des services Cloud; cependant ce changement d'utilisation des ressources informatiques nécessite une formation et un accompagnement des métiers.

Il est donc indispensable d'être accompagné d'un partenaire de confiance, capable d'accompagner le changement technique par un changement des mentalités, avec le soutien des dirigeants.

Au final, la construction d'un écosystème technique de confiance Cloud est une étape structurante et indispensable pour toute entreprise : il s'agit du premier pas pour reconquérir la confiance des utilisateurs, et permettre à l'entreprise de découvrir de nouveaux cieux.

[30] Agence Nationale de la Sécurité des Systèmes d'Information

Références

- **Louis Naugès,** *Moderniser son Système d'Information: le modèle B I S, Business, Infrastructures, Support*. http://nauges.typepad.com/my_weblog/2015/01/moderniser-son-syst%C3%A8me-dinformation-le-mod%C3%A8le-bis-business-infrastructures-support.html
- **Louis Naugès**, *Les métiers des services IT vont être chamboulés par le cloud* - http://www.informatiquenews.fr/metiers-services-etre-chamboules-cloud-louis-nauges-consultant-47927
- **AngelList**, *relevé effectué le 04/11/2016* - https://angel.co/saas
- **GetApp.com**, *relevé effectué le 03/11/2016* - https://www.getapp.com/
- **Synergy Research Group**, *Microsoft is on a Charge in the SaaS Market* - https://www.srgresearch.com/articles/microsoft-charges-ahead-saas-market
- **Gartner**, *Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach $204 Billion in 2016* - http://www.gartner.com/newsroom/id/3188817
- **Kenneth Corbin**, *CIOs vastly underestimate extent of shadow IT* - http://www.cio.com/article/2968281/cio-role/cios-vastly-underestimate-extent-of-shadow-it.html
- **Tony Kontzer**, *Shadow IT's Growing Footprint* - http://www.cioinsight.com/security/slideshows/shadow-its-growing-footprint.html
- **Ariane Beky**, *Shadow IT : la DSI ne doit plus être le « ministère du non »* - http://www.silicon.fr/shadow-it-dsi-ministere-non-154198.html
- **LaRevueDuDigital**, *Le Shadow IT, créateur de solutions entre la DSI et le métier chez Saint Gobain* - http://www.larevuedudigital.com/2016/03/26/le-shadow-it-createur-de-solution-entre-la-dsi-et-le-metier-chez-saint-gobain/
- **Alain Clapaud**, *Saint-Gobain élargit sa stratégie multi-Cloud* - http://www.lemagit.fr/etude/Saint-Gobain-elargit-sa-strategie-multi-Cloud
- **CornerstoneOnDemand**, *Saint-Gobain s'appuie sur le cloud de Cornerstone OnDemand pour ouvrir ses formations à tous ses collaborateurs* - https://www.cornerstoneondemand.fr/company/news/press-releases/saint-gob

ain-s%e2%80%99appuie-sur-le-cloud-de-cornerstone-ondemand-pour-ouvrir-ses

- **Anthony Sollinger**, *Cloud computing : donner plus de visibilité pour construire un vrai climat de confiance* - http://www.journaldunet.com/solutions/expert/65431/cloud-computing---donner-plus-de-visibilite-pour-construire-un-vrai-climat-de-confiance.shtml
- **Dave Key**, *Requirements for Enterprise SaaS Applications* - http://cloudstrategies.biz/requirements-for-building-enterprise-saas-applications/
- **McAfee**, *Infographic : The Hidden Truth behind Shadow IT* - http://www.mcafee.com/cn/resources/misc/infographic-shadow-it.pdf
- **Andrew Froelich**, *Shadow IT: It's Much Worse Than You Think* - http://www.informationweek.com/cloud/shadow-it-its-much-worse-than-you-think/a/d-id/1321637
- **Gartner**, *Cloud Access Security Brokers* - http://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs/
- **Gartner**, *How to evaluate and operate a Cloud Access Security Broker* - http://info.skyhighnetworks.com/WP-Gartner-How-to-Evaluate-a-CASB_Banner-Cloud.html?Source=website&LSource=website
- **iVision**, *Shadow IT : Les risques et les opportunités de l'Informatique fantôme* - http://www.ivision.fr/shadow-it-les-risques-et-les-opportunites-de-linformatique-fantome/
- **Bureau Veritas**, Etude Databerg - http://images.info.veritas.com/Web/Veritas/%7B364a7ca5-e05c-4fce-971b-88e18c62eafb%7D_45145_EMEA_Veritas_Strike_Report_Gulf.pdf