Rapport

Ciel dégagé à l'horizon ?

Le point sur l'adoption du cloud

intel Security

Sommaire

Nous tenons à remercier les 1 200 personnes interrogées pour leur participation à notre enquête, de même que les cadres supérieurs suivants qui, par leur expertise et leurs réflexions, ont contribué à l'élaboration de ce rapport :

- Brent Conran, Vice-Président et Responsable de la sécurité des systèmes d'informations, Intel
- Brian Dye, Vice-Président de groupe, Intel Security
- Dimitra Liveri, Responsable de la sécurité des réseaux et des informations, ENISA (European Network and Information Security Agency)
- Vanessa Pegueros, Responsable de la sécurité des systèmes d'informations, DocuSign, Inc.
- Jim Reavis, Président-Directeur Général, Cloud Security Alliance
- Dave Shackleford, Analyste SANS et PDG, Voodoo Security
- Timothy Youngblood, Responsable de la sécurité des systèmes d'informations, Kimberly-Clark

Un cloud universel ? Une question de confiance

Chaque fois que nous allumons un appareil électronique, nous nous retrouvons quasiment tous face au « cloud computing » (ou informatique distribuée), sous une forme ou une autre. Qu'il s'agisse d'applications domotiques ou métier génératrices de revenus, nous dépendons tous d'Amazon Web Services, Microsoft Azure et d'autres fournisseurs de services de cloud qui assurent la disponibilité de ces services. À l'heure où nous examinons l'évolution et l'avenir du cloud computing, force est d'admettre que notre utilisation de cette plate-forme informatique est vouée à croître et que notre dépendance vis-à-vis du cloud aura des conséquences majeures pour chacun d'entre nous, particuliers comme entreprises. D'après notre enquête, l'essentiel du budget informatique des entreprises au cours des 12 à 18 prochains mois sera consacré à des ressources de cloud public. D'aucuns considèrent que nous sommes à un tournant de l'histoire de l'informatique.

Examinons d'un peu plus près les implications de cette transition. Tout d'abord, les professionnels des technologies qui travaillent au sein de ces entreprises vont devoir développer considérablement leurs compétences. Ensuite, le degré de confiance dans le cloud devra s'améliorer, de même que la visibilité supplémentaire dont nous avons tous besoin pour parvenir à ce niveau de confiance.

Si le cloud est d'ores et déjà une réalité, l'avenir promet une expansion de ses capacités, et il ne serait pas surprenant de voir des applications et services d'infrastructure critiques migrer vers le cloud. En effet, à l'heure où nous commençons à formuler des hypothèses sur ce à quoi ressemblera le centre de données du futur, il n'est pas déraisonnable d'envisager la généralisation d'une approche de type « le cloud avant tout », dans le cadre de laquelle les applications seront déployées dans le cloud par défaut, et où l'hébergement sur site (pourvu qu'il soit justifié) représentera l'exception.

Avec le niveau de sécurité approprié, la puissance du cloud computing peut être exploitée pour prendre en charge de nouvelles applications et des outils métier avancés permettant d'améliorer la productivité. Néanmoins, comme vous le découvrirez à la lecture de notre étude, les entreprises continuent de se heurter à des problèmes de confiance et de sécurité.

La généralisation progressive de l'adoption du cloud nous offre l'opportunité de renforcer la confiance dans cette technologie afin de répondre aux attentes des entreprises et des particuliers. La CSA (Cloud Security Alliance), une organisation à la pointe de la recherche technique dirigée par des bénévoles, invite les entreprises et leurs utilisateurs à devenir acteurs et leaders de cette révolution.

— Raj Samani, Directeur des Technologies EMEA, Intel Security
— Jim Reavis, PDG, Cloud Security Alliance

Introduction

Les besoins métier poussent rapidement les entreprises vers le cloud, au-delà des pilotes et des projets de petite envergure. Dans ce contexte, il convient d'examiner les tendances clés et les défis auxquels elles seront confrontées. En d'autres termes, comment les entreprises peuvent-elles tirer le meilleur parti du cloud sans compromettre la sécurité et le contrôle ?

Au cours d'une enquête menée dans huit pays, nous avons interrogé 1 200 décideurs informatiques chargés de la sécurité dans le cloud au sein de leur entreprise sur leurs plans en matière d'adoption du cloud, leurs principaux défis et leurs priorités en matière d'investissement pour l'année à venir.

Dans ce rapport, nous analysons les tendances en matière d'adoption du cloud et leur ventilation entre services de logiciels (SaaS, Software-as-a-Service), d'infrastructure (IaaS, Infrastructure-as-a-Service), de plate-forme (PaaS, Platform-as-a-Service) et de sécurité (Security-as-a-Service), ainsi qu'entre clouds publics, privés et hybrides. Nous nous penchons également sur la façon dont les entreprises des secteurs plus réglementés tentent de surmonter les problèmes de conformité liés à l'adoption du cloud.

« Nous avons largement dépassé le cercle réduit des entreprises intéressées par les technologies de pointe — celles qui testent et pilotent l'évolution du cloud — pour atteindre le stade de l'adoption pleine et entière de toute une série de types de cloud différents. Aujourd'hui, nous observons une reconnaissance à tous les niveaux que le cloud représente l'avenir de l'informatique, et que nous assistons à la mutation de l'informatique en service utilitaire. »

— Jim Reavis, PDG,
Cloud Security Alliance

Nous examinons par ailleurs les mythes et la réalité des principaux problèmes de sécurité du cloud auxquels sont confrontées les entreprises, et nous penchons sur l'efficacité des investissements dans les technologies de protection du cloud, telles que le chiffrement, la prévention des fuites de données, etc.

Nous nous intéressons également à la manière dont les entreprises répondent au défi posé par les applications de cloud relevant de l'informatique de l'ombre tout en permettant à leurs employés et départements d'accéder aux services dont ils ont besoin, avec la sécurité nécessaire pour protéger les informations d'entreprise. Enfin, nous évaluons le degré de sensibilisation des dirigeants d'entreprises aux risques de sécurité liés au cloud.

Les services informatiques d'entreprise renforcent leurs investissements dans le cloud

Le cloud fait d'ores et déjà partie de la vie des particuliers, qui l'utilisent au quotidien pour accomplir des tâches telles que télécharger des photos, accéder à leur messagerie électronique ou sauvegarder des données. Notre enquête montre que nous sommes aujourd'hui en passe d'atteindre un point d'inflexion comparable, où le cloud deviendra un objectif technologique prédominant pour les services informatiques d'entreprise.

Si la progression de l'adoption du cloud par les entreprises et l'augmentation des investissements dans cette technologie ne sont pas réellement une surprise, la rapidité à laquelle cette évolution se produit est en revanche particulièrement remarquable. Notre enquête met toutefois en lumière un changement de stratégie notable de la part des services informatiques d'entreprise, puisque dans moins de 18 mois, et parfois même plus rapidement pour certains pays, la grande majorité des entreprises consacreront l'essentiel de leur budget informatique à des services de cloud (Figure 1). Les participants s'attendent à ce que, d'ici 16 mois, 80 % du budget informatique de leur entreprise soit alloué à des services de cloud. Les entreprises brésiliennes et australiennes prévoient d'atteindre ce seuil dans les 12 prochains mois.

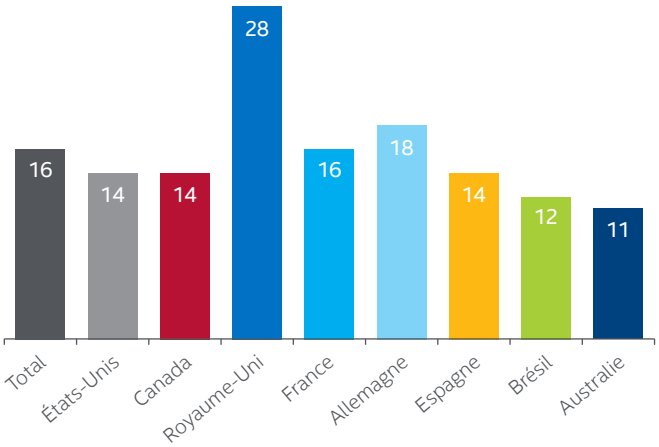

Figure 1. Nombre moyen de mois avant que 80 % du budget informatique de l'entreprise du participant soient dédiés à des services de cloud, par pays

« Nos partenaires commerciaux tirent parti de la nature dynamique du cloud, de la vitesse accrue, du renforcement de la collaboration et de l'élasticité des services — autant d'éléments qui participent à l'attrait du cloud — et prennent des mesures pour amplifier tous ces aspects et éviter de se retrouver à la traîne. En tant que professionnels de la sécurité, nous devons faire preuve d'engagement et montrer que la sécurité peut créer de nouvelles perspectives. »

— Timothy Youngblood, RSSI,
Kimberly-Clark

La migration vers les services de cloud citée par les participants à l'enquête consistera en des déploiements de clouds publics et privés. Selon les résultats de notre enquête, le cloud privé constitue le modèle de cloud prédominant au sein des entreprises (51 % de tous les déploiements dans le cloud). Le cloud public représente quant à lui 30 % des déploiements dans le cloud des entreprises, et le cloud hybride 19 %. Si l'on examine de plus près le temps qu'il faudra pour que 80 % du budget informatique d'une entreprise soit alloué à des services de cloud, le délai se réduit à seulement 15 mois lorsqu'il s'agit de cloud privé.

« DocuSign a fait sienne la philosophie du "cloud avant tout", et nous voyons un grand nombre de nos clients adopter une approche similaire. Il est plus difficile de convaincre les entreprises issues de secteurs très réglementés, tels les services financiers ou les soins de santé. Les services informatiques de ces entreprises sont dans une position très délicate car les organismes de réglementation dont ils dépendent exigent qu'ils prouvent que toutes les mesures de sécurité sont en place avant l'implémentation. Ils sont donc mis à rude épreuve puisque, d'une part, ils doivent prendre le temps de prouver à ces organismes que toutes les mesures de sécurité nécessaires ont été prises et que, d'autre part, leur entreprise les exhorte à faire montre d'une efficacité et d'une agilité toujours plus grandes, toujours plus vite. »

— Vanessa Pegueros, RSSI, DocuSign, Inc.

« Il convient d'être attentif aux informations qui peuvent être hébergées dans le cloud ou qui doivent au contraire être stockées en interne. Si vous êtes en présence d'informations de grande valeur pour l'entreprise, il est sans doute préférable qu'elles ne sortent pas du périmètre de l'entreprise et soient hébergées dans un cloud privé. »

— Eric Knapp, Directeur mondial de la cybersécurité, Honeywell

Les informations recueillies indiquent que l'adoption des services de cloud a véritablement atteint un point de basculement. À l'heure actuelle, les entreprises utilisent en moyenne 43 services de cloud, même si certaines variations régionales notables sont à signaler (Figure 2). Ainsi, le Royaume-Uni est à la traîne avec seulement 29 services de cloud par entreprise en moyenne, tandis que les entreprises brésiliennes comptent parmi les plus enthousiastes (55 services de cloud par entreprise).

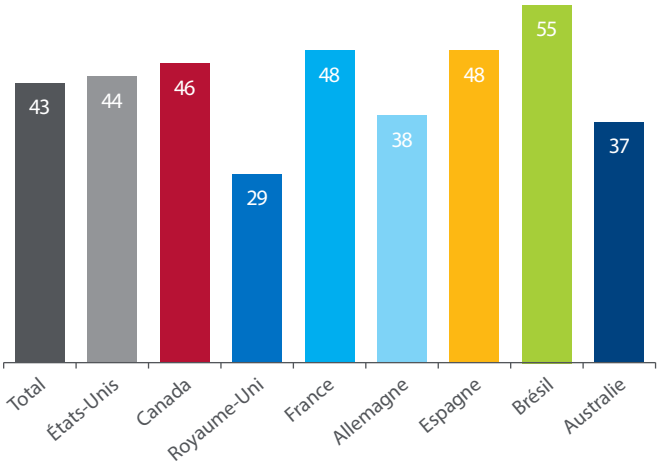

Figure 2. Nombre moyen de services de cloud utilisés par les entreprises, par pays

Bien entendu, il y aura également des différences au niveau du taux d'adoption des différents types de plate-formes de cloud — cloud public, privé, hybride ou géré, ou encore SaaS, IaaS et PaaS. D'après nos observations, le degré d'adoption varie en outre d'un secteur à l'autre. Ainsi, dans les secteurs très réglementés tels que les services financiers, la migration vers le cloud suscite encore des réticences. De même, le secteur public et les administrations accusent un certain retard.

Lorsque l'on examine les tendances en matière d'adoption du cloud, il peut être tentant de se limiter à parler des services SaaS. Or notre enquête révèle que, si la majorité des entreprises prévoient d'investir dans les différents modèles de services de cloud, ce sont en réalité (ce qui peut surprendre) les services IaaS qui enregistrent le pourcentage d'intention le plus élevé (81 %), contre 60 % seulement pour les services SaaS (Figure 3). Ils sont suivis de près par les services de sécurité (Security-as-a-Service) (79 %), et mêmes les investissements prévus dans les services PaaS (69 %) sont supérieurs aux services SaaS.

Ces chiffres sont confirmés par le rapport du SANS Institute, qui indique également que les services IaaS représenteront le principal secteur de croissance en termes de déploiements dans le cloud d'entreprise au cours des 12 prochains mois.

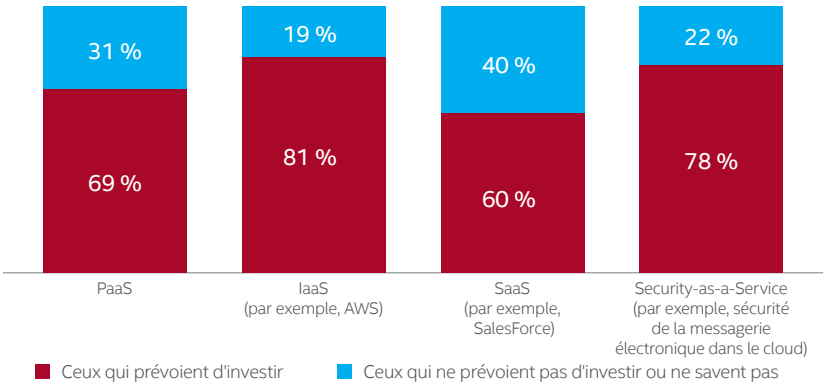

Figure 3. Dans quels types de déploiements dans le cloud votre entreprise prévoit-elle d'investir ?

« Le manque de visibilité sur la manière dont opère le fournisseur de services de cloud et sur les événements qui surviennent entrave véritablement l'analyse des risques et la prise de décisions en matière de gestion des risques. De nombreuses réglementations sont antérieures à l'apparition du cloud et reposent sur l'hypothèse qu'une entreprise exerce un contrôle total sur les technologies informatiques, ce qui n'est plus le cas avec le cloud. »

— Jim Reavis, PDG,
Cloud Security Alliance

« Les compromissions de données suscitent de vives inquiétudes. De nombreuses attaques ciblent les informations d'identification des utilisateurs disposant d'un accès légitime au service de cloud. C'est ainsi que les informations sont exfiltrées. »

— Jim Reavis, PDG,
Cloud Security Alliance

Sécurité et conformité : la nécessité d'une meilleure visibilité

Quelles sont les implications de cette généralisation de l'adoption du cloud pour la sécurité des entreprises ? Le nombre de données sensibles importantes hébergées dans le cloud devrait augmenter considérablement. Quelque 40 % des participants à l'enquête **Orchestrating Security in the Cloud** (Coordonner la sécurité dans le cloud) réalisée par le SANS Institute indiquent qu'ils traitent ou stockent des données sensibles dans le cloud[1]. Les types de données les plus fréquemment stockés dans le cloud sont des données de veille économique (52 %), des données financières et comptables (52 %), des dossiers d'employés (48 %) et des données personnelles de clients (40 %). 13 % des entreprises ont déclaré ne pas savoir si elles possèdent des données sensibles dans le cloud, ce qui est particulièrement préoccupant. De nombreux experts pensent que ce chiffre est en réalité bien plus élevé, surtout parmi les entreprises de grande taille. En effet, certaines entreprises refusent d'admettre leur ignorance, tandis que d'autres ne savent pas si elles sont exposées de la sorte en raison de la dissémination de leurs opérations et de leurs divisions aux quatre coins du monde.

72 % des participants à l'enquête du SANS Institute indiquent que le maintien de la conformité dans le cloud constitue leur principale préoccupation, indépendamment du type de déploiement dans le cloud. La visibilité constitue un véritable défi. En effet, plus de la moitié (58 %) des participants à l'enquête du SANS Institute citent le manque de visibilité sur les opérations des fournisseurs de services de cloud comme principal problème.

Des nuages à l'horizon ? Menaces pour le vingt-et-unième siècle

Le fossé entre la perception et la réalité révélé par notre enquête suggère qu'il est temps de réévaluer les menaces qui pèsent véritablement sur le cloud.

Dans la plupart des pays, la principale préoccupation liée à l'utilisation de services SaaS concerne les incidents de sécurité touchant les données, comme indiqué par plus d'un répondant sur cinq (22 %). Les compromissions de données arrivent également en tête des préoccupations pour ce qui est des services IaaS et des clouds privés. Il existe cependant des différences régionales, plus particulièrement en Australie, où l'indisponibilité des services constitue la principale préoccupation.

Mais qu'en est-il vraiment ?

Lorsqu'elles sont interrogées plus avant, moins d'un quart (23 %) des entreprises déclarent avoir effectivement subi une fuite ou une compromission de données hébergées par leurs fournisseurs de services de cloud. Et seulement une sur cinq indique avoir été victime d'un accès non autorisé à ses données ou services. L'enquête du SANS Institute fait apparaître un taux de compromissions des données hébergées dans le cloud plus faible encore. En effet, seuls 9 % des entreprises interrogées ont été victimes d'un incident dans des clouds publics ou dans des applications SaaS ou du cloud privé.

Les principaux incidents et problèmes liés à l'utilisation des services de cloud mentionnés par les participants à l'enquête concernaient la migration des services et des données, les coûts élevés/ la faible valeur et le manque de visibilité sur les opérations des fournisseurs de services de cloud (Figure 4).

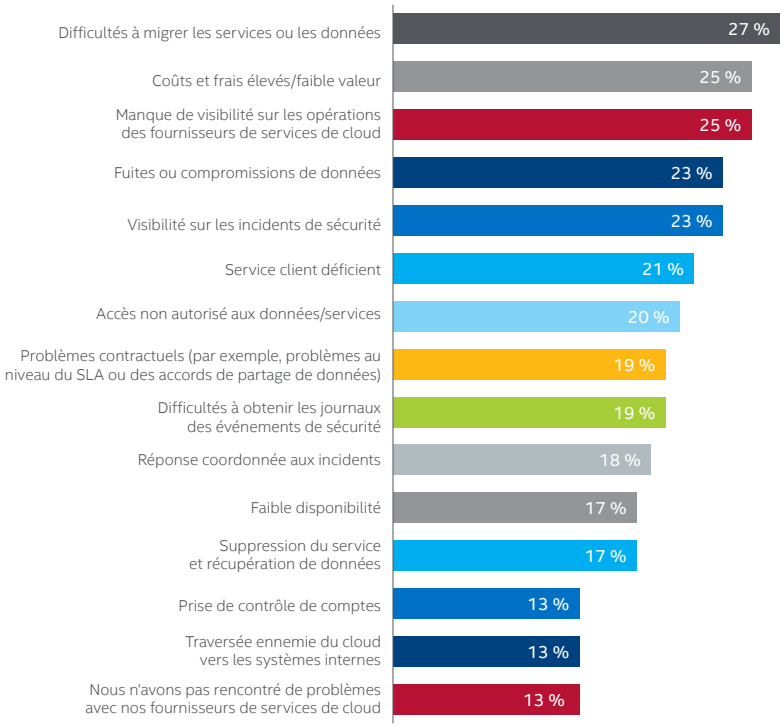

Figure 4. Eu égard à la sécurité du cloud, quels problèmes votre entreprise a-t-elle rencontrés dans le cadre de ses relations avec des fournisseurs de services de cloud ?

Parmi les menaces de sécurité spécifiques au cloud identifiées par les participants à l'enquête, les logiciels malveillants (malware) et les réseaux de robots (botnets) arrivent en tête pour les déploiements de cloud privé (33 %), tandis que les attaques par déni de service sont perçues comme la principale menace ciblant les clouds publics (36 %).

« Les entreprises doivent intégrer la sécurité dans les tâches DevOps et les deux éléments les plus critiques sont la surveillance en continu et la détection des modifications. »

— Dave Shackleford, Analyste SANS et PDG, Voodoo Security

L'expansion ou la réduction rapide des services peut également engendrer d'autres risques de sécurité liés au cloud, même s'il s'agit davantage d'un problème de disponibilité et de continuité des activités que doivent prendre en compte les entreprises. L'adoption du cloud est également à l'origine de la montée en puissance des DevOps, en raison de l'accélération des cycles de développement, de test et de déploiement d'applications. L'intégration d'une sécurité robuste dans cet environnement de développement continu est essentiel pour les entreprises, si elles veulent pouvoir suivre ces modifications rapides et être informées des risques de sécurité potentiels associés à ces modifications.

Il va sans dire que les résultats de l'enquête ne doivent pas nous amener à conclure que les compromissions de données hébergées dans le cloud ne constituent pas une menace de sécurité sérieuse, ou qu'elles n'arrivent jamais. Nous devons envisager la possibilité que les compromissions de données qui ne sont pas divulguées aux autorités policières ou aux organismes de réglementation soient passées sous silence. De plus, les conséquences d'une compromission de données hébergées dans le cloud sont souvent considérables. Il est clair que le fossé entre la perception et la réalité des menaces de sécurité liées au cloud se doit d'être comblé. L'enquête laisse toutefois entendre que les investissements et les efforts de planification visant à réduire les risques de compromissions de grande envergure doivent être mis en balance avec certaines menaces plus courantes auxquelles sont exposés au quotidien les systèmes d'entreprise et les données dans le cloud. Ces menaces peuvent notamment prendre la forme de problèmes de migration, d'un service clients déficient et de problèmes contractuels, ou encore de menaces de sécurité spécifiques telles que les attaques par déni de service, les logiciels malveillants et le piratage de comptes.

Gestion de la sécurité et des risques liés au cloud : les œillères des cadres dirigeants

« Les conseils d'administration et les cadres dirigeants reconnaissent pour la plupart que la sécurité du cloud constitue un élément crucial pour toute entreprise et doit être prise au sérieux. »

— Vanessa Pegueros, RSSI, DocuSign, Inc.

Notre enquête révèle un degré élevé d'implication des cadres dirigeants dans le processus de prise de décisions en matière de sécurité dans le cloud, qui ne se limite pas au directeur informatique, au directeur des systèmes d'informations et au responsable de la sécurité des systèmes d'informations, mais inclut également souvent le PDG et le directeur financier. On peut toutefois se demander si les cadres dirigeants prennent véritablement la mesure des risques de sécurité associés au cloud.

Ainsi, il semble que les dirigeants n'aient pas réellement conscience des risques de sécurité associés au stockage de données sensibles dans le cloud public. (Voir la Figure 5.) Seuls 34 % des participants à l'enquête estiment que les cadres dirigeants de leur entreprise comprennent parfaitement ces risques, et pour un répondant sur cinq, les dirigeants de l'entreprise ne comprennent que partiellement ces risques ou n'en ont aucune conscience. Cette méconnaissance est encore plus prononcée au Royaume-Uni, puisque seuls 15 % des participants à l'enquête pensent que les cadres dirigeants de leur entreprise comprennent parfaitement les risques associés au stockage de données sensibles dans le cloud public. Le degré de compréhension des risques par les cadres dirigeants est nettement supérieur au Brésil (49 %) et en Australie (47 %).

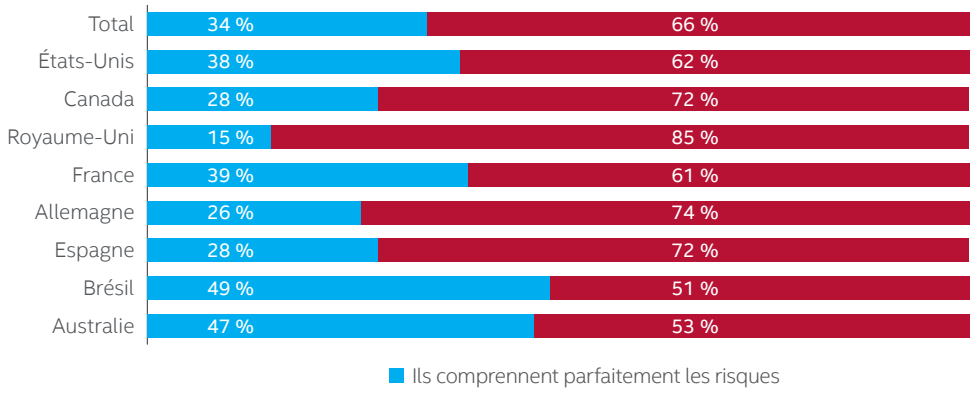

Figure 5. Pensez-vous que les cadres dirigeants/la direction de votre entreprise comprennent les risques de sécurité associés au stockage de données sensibles dans le cloud public ?

Si les compromissions de données médiatisées et leurs conséquences en termes financiers et de réputation ont fait de la sécurité des données une des priorités de nombreux PDG et cadres dirigeants, notre enquête met en évidence la nécessité de renforcer la sensibilisation aux risques associés au stockage de données sensibles dans le cloud.

Informatique de l'ombre : risque ou opportunité ?

« Savoir, c'est pouvoir. Nous avons mis en place un programme intensif de sensibilisation à la sécurité qui s'attache à enseigner à tous nos employés la valeur des informations. C'est ce que j'appelle notre "pare-feu humain". »

— Timothy Youngblood, RSSI, Kimberly-Clark

Pour la majorité des participants à notre enquête, l'informatique de l'ombre a un impact négatif sur la capacité de leur entreprise à préserver la sécurité des services de cloud ; 10 % d'entre eux indiquent même qu'elle expose leur entreprise à un risque élevé.

La sécurité de l'informatique de l'ombre continue de représenter un défi majeur : 52 % des départements d'entreprise attendent du service informatique qu'il protège les services de cloud non autorisés qu'ils ont déployés. En outre, d'après près d'un quart des participants à l'enquête (23 %), ces départements mettent en œuvre leurs propres solutions de sécurité sans l'aide du service informatique.

La visibilité sur les services non approuvés mis en œuvre par les départements est généralement meilleure pour les services SaaS que pour les services IaaS. Cependant, au moins un cinquième des participants à notre enquête ignorent l'ampleur de ce phénomène au sein de leur entreprise.

« L'informatique de l'ombre constitue le nouveau modèle informatique. L'ancien modèle est mort. Plus nous la combattons, plus nous détournons notre attention de la nécessité de la sécuriser. Nous devons accepter que l'informatique de l'ombre fait partie de la réalité d'aujourd'hui et consacrer notre énergie à la gérer en toute sécurité. »

— Vanessa Pegueros, RSSI, DocuSign, Inc.

« Les gens essaient juste de faire leur travail. Si nous ne pouvons pas leur fournir les outils qui leur permettront de le faire, ils iront les chercher ailleurs. Le service informatique et le directeur informatique doivent servir d'intermédiaires et adopter les services de cloud et SaaS. »

— Brent Conran, Vice-Président et RSSI, Intel

L'informatique de l'ombre est particulièrement répandue au sein des départements marketing, R&D et des ventes. Le principal point d'interrogation concerne le service juridique. Quelque 37 % des participants à l'enquête ne sont pas en mesure de déterminer si celui-ci utilise des services de cloud à l'insu du service informatique.

Comment les entreprises s'attaquent-elles à l'informatique de l'ombre ? Les méthodes les courantes sont les suivantes :

- Surveillance de l'activité des bases de données (49 %)
- Firewalls NG (41 %)
- Passerelles web (37 %)

Une autre tactique consiste à collaborer avec le service financier afin d'être informé de toute note de frais concernant des services de cloud.

Lorsque des services non approuvés sont mis au jour, les services informatiques ont tendance à adopter deux types de mesures diamétralement opposés. Près de la moitié des participants à l'enquête (46 %) bloquent l'accès, tandis que 37 % migrent ces applications vers un service approuvé.

La confiance dans le cloud s'améliore-t-elle ?

De prime abord, les principaux chiffres de notre enquête indiquent un degré de confiance dans le cloud relativement faible par rapport à l'informatique hébergée sur site ou en interne. Sans surprise, le cloud public est le modèle qui inspire le moins confiance (Figure 6).

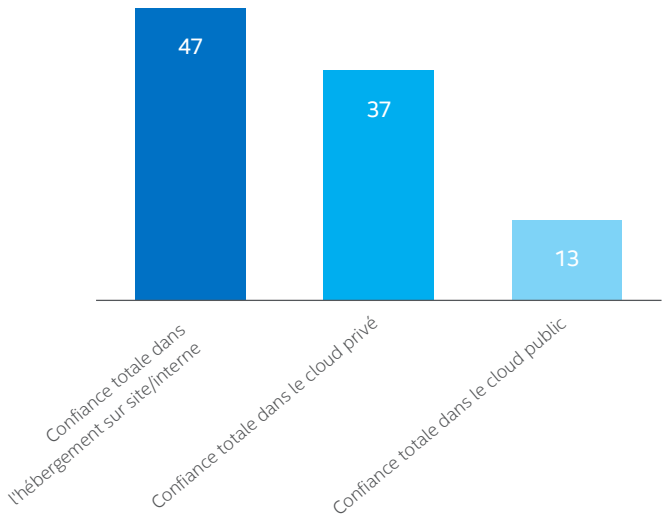

Figure 6. Dans quelle mesure feriez-vous confiance aux modèles suivants pour assurer la sécurité de vos données sensibles ?

On notera toutefois avec intérêt un renforcement de la confiance dans le cloud au cours de l'année écoulée. En effet, 77 % des participants à l'enquête affirment que leur entreprise a davantage confiance dans le cloud aujourd'hui qu'il y a un an (Figure 7).

« Nous sommes à l'aube d'une nouvelle ère pour les fournisseurs de services de cloud. Nous sommes actuellement en période de transition, mais je pense que ces nouvelles dispositions réglementaires favoriseront les investissements et la confiance, ce qui nous permettra de nous sentir plus à l'aise vis-à-vis des services de cloud. »

— Dimitra Liveri, Responsable de la sécurité des réseaux et des informations, ENISA (Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information)

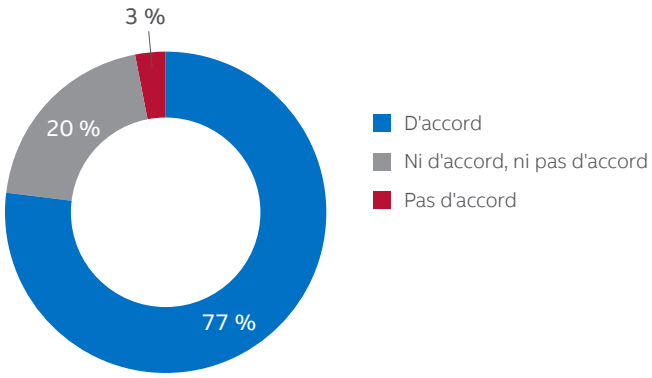

Figure 7. Pourcentage de participants d'accord avec l'affirmation « Mon entreprise a plus confiance dans le cloud qu'il y a 12 mois. »

Avec deux réglementations majeures sur le point d'être votées par la Commission européenne, 2016 promet d'être une année cruciale pour les fournisseurs de services de cloud et leurs utilisateurs. Il s'agit, d'une part, du règlement général sur la protection des données (RGPD) et, d'autre part, de la directive sur la sécurité des réseaux et de l'information (SRI). Ces réglementations contribueront-elles à enforcer la confiance dans la sécurité du cloud ? Les experts pensent que oui.

Priorités d'investissement en matière de sécurité du cloud

Les priorités d'investissement en matière de sécurité varient selon le type de déploiement dans le cloud. En moyenne, les entreprises recourent à trois solutions de sécurité pour protéger leurs applications SaaS. Les plus courantes sont les solutions de chiffrement des fichiers (60 %), suivies des solutions de sécurité de la messagerie électronique (55 %).

Pour assurer la protection de leurs services IaaS, les entreprises utilisent en moyenne quatre solutions de sécurité. Les plus courantes sont les pare-feux (70 %) et les solutions de chiffrement (62 %). Le cloud privé entraîne également le déploiement de quatre solutions de sécurité en moyenne, pare-feux en-tête (67 %).

Les quatre principaux aspects de la sécurité en tant que service dans lesquels les entreprises prévoient d'investir sont ceux dans lesquels elles investissent déjà : la protection de la messagerie, la protection de l'environnement web, la protection antimalware et la protection des applications par pare-feu (Figure 8). Cette tendance indique que les entreprises prévoient d'améliorer et d'étendre les services de sécurité dans le cloud déjà en place.

L'enquête du SANS Institute met également en lumière plusieurs aspects clés de la sécurité du cloud qui feront l'objet d'investissements au cours des 18 prochains mois. Il s'agit notamment de l'analyse des vulnérabilités, de l'authentification multifacteur, de la prévention des fuites de données, de la gestion des journaux, des systèmes de détection des intrusions (IDS) et de prévention des intrusions (IPS), des systèmes de gestion des événements et des informations de sécurité (SIEM) et des services de contrôle CASB (Cloud Access Security Brokers).

D'après le rapport *Market Guide for Cloud Access Security Brokers* (Guide du marché des intermédiaires de sécurité de l'accès au cloud) de Gartner, les services CASB en particulier représentent un secteur à forte croissance. Gartner prédit qu'« en 2020, 85 % des grandes entreprises utiliseront une solution CASB pour leurs services de cloud, contre moins de 5 % aujourd'hui »[2]. Notre enquête tend à confirmer ces prévisions. Bien que les services CASB soient relativement récents, 36 % des entreprises y ont recours pour assurer la protection de leurs applications SaaS, et 32 % les utilisent pour surveiller les implémentations de cloud relevant de l'informatique de l'ombre. Près d'un quart (24 %) des entreprises prévoient également d'investir dans une solution CASB sous forme de service dans un avenir plus ou moins proche.

« La première question à se poser en matière de sécurité des entreprises dans le cloud public est la suivante : quelles sont les limites de la responsabilité ? Qu'êtes-vous en mesure de contrôler en tant qu'entreprise et quels sont les éléments qui doivent nécessairement être gérés par le fournisseur de services de cloud ? Vous devez ensuite évaluer les contrôles sur tout le spectre de la sécurité, notamment la sécurité des données, la gestion des identités et l'application des stratégies. Il y a des choses que vous ne pourrez plus contrôler, en particulier au niveau du réseau. »

— Dave Shackleford, Analyste SANS et PDG, Voodoo Security

« Il est absolument crucial de comprendre ce qui se passe dans votre environnement de cloud, par exemple entre la base d'utilisateurs et SalesForce. Je compte donc m'intéresser davantage aux outils qui nous permettent de gérer ces événements de façon plus sécurisée. Nous avons également besoin d'outils permettant d'automatiser les processus, tels que la réponse aux incidents, et de faire plus avec ceux dont nous disposons actuellement. »

— Vanessa Pegueros, RSSI, DocuSign, Inc.

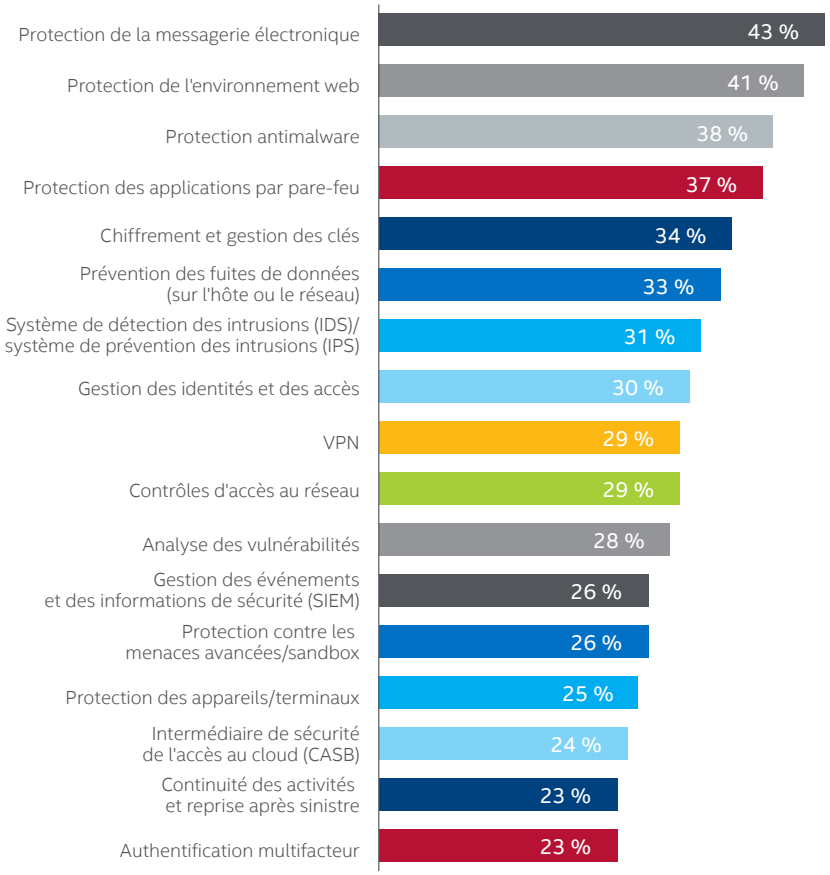

Figure 8. Dans quels domaines de la sécurité sous forme de service (Security-as-a-Service) votre entreprise prévoit-elle d'investir ?

Parmi les entreprises qui utilisent un service de cloud public, un peu plus d'un tiers (34 %) indiquent disposer d'une solution unifiée avec intégration complète et gestion centralisée des systèmes hybrides hébergés sur site et dans le cloud. La marge de progression est donc loin d'être négligeable.

En résumé

L'adoption du cloud dans l'entreprise se rapproche à grands pas d'un point de basculement, puisque les entreprises affirment que dans 16 mois ou moins, 80 % de leur budget informatique sera consacré à des services de cloud.

De nombreux incitants puissants poussent les entreprises vers le cloud, notamment la flexibilité accrue, les innovations plus rapides et la réduction des coûts. Cependant, les nombreuses options de déploiement dans le cloud apportent inévitablement leur lot de défis de sécurité. Dans la mesure où le cloud est ou sera dépositaire d'un volume considérable de données métier critiques, les entreprises doivent tenir compte des aspects suivants :

- La responsabilité des contrôles de sécurité et de la conformité est partagée par les entreprises et les fournisseur de services de cloud. Interrogez votre fournisseur de services sur les contrôles de sécurité qu'il a mis en place et assurez-vous que votre accord de niveau de service (SLA) prévoit la génération de rapports. Il est néanmoins essentiel que l'entreprise sécurise les éléments dont elle a le contrôle dans le cloud, qu'il s'agisse des données, des applications ou des charges de traitement, et qu'elle intègre la sécurité dans son projet d'architecture de cloud.

« La délocalisation et le recours au cloud ne signifient pas que vous externalisez votre responsabilité. Vous ne pouvez pas dire "Ce n'est pas moi, c'est Amazon !". »

— Brent Conran, Vice-Président et RSSI, Intel

- Les principaux domaines où sont consentis des investissements de sécurité sont le chiffrement de données, la gestion des identités et des accès, la prévention des fuites de données et la protection de la messagerie électronique. Les entreprises investissent également de plus en plus dans la sécurité sous forme de service (Security-as-a-Service) et dans d'autres services permettant de coordonner la sécurité entre plusieurs fournisseurs et environnements, en particulier les services CASB.
- Si les déploiements de cloud relevant de l'informatique de l'ombre continuent de représenter un défi majeur dans la mesure où ils peuvent exposer les données d'entreprise à un risque accru, les services informatiques doivent collaborer avec les différents départements pour trouver un moyen plus sécurisé de permettre aux utilisateurs d'implémenter leurs propres déploiements de cloud. Le service informatique pourrait reprendre le contrôle et bénéficier d'une meilleure visibilité en servant d'intermédiaire et en orientant les utilisateurs de l'entreprise vers des services de cloud plus sécurisés.
- Malgré l'implication croissante de nombreux cadres dirigeants dans le processus décisionnel en matière de sécurité dans le cloud, leur degré de sensibilisation et leur compréhension des risques associés au cloud sont clairement insuffisants. Une plus grande sensibilisation est nécessaire, de même qu'une participation accrue des DSI et des RSSI aux réunions du conseil d'administration avec les autres cadres dirigeants. Les répercussions financières et les atteintes à la réputation subies par certaines entreprises lors de récentes compromissions de données très médiatisées doivent inciter les dirigeants à faire de la sécurité des données une priorité, qu'elles soient hébergées en interne ou dans le cloud.

Méthodologie

L'enquête auprès de 1 200 responsables informatiques chargés de la sécurité du cloud au sein de leur entreprise a été réalisée par Vanson Bourne en juin 2015. Les participants étaient issus d'Allemagne, d'Australie, du Brésil, du Canada, d'Espagne, des États-Unis, de France et du Royaume-Uni, et d'un large éventail de moyennes (de 251 à 500 employés) et grandes entreprises (plus de 5 000 employés).

À propos d'Intel Security

McAfee fait désormais partie d'Intel Security. Avec sa stratégie Security Connected, son approche innovante de la sécurité optimisée par le matériel et son réseau mondial de cyberveille sur les menaces Global Threat Intelligence, Intel Security met tout en œuvre pour proposer des solutions et des services de sécurité proactifs et éprouvés, qui assurent la protection des systèmes, réseaux et équipements mobiles des entreprises et des particuliers du monde entier. Intel Security associe le savoir-faire et l'expérience de McAfee aux innovations et aux performances reconnues d'Intel pour faire de la sécurité un élément essentiel de chaque architecture et plate-forme informatique. La mission d'Intel Security est de permettre à chacun de vivre et de travailler en toute confiance et en toute sécurité dans le monde numérique. **www.intelsecurity.com**

1. *SANS : Orchestrating Security in the Cloud* (Coordonner la sécurité dans le cloud), Dave Shackleford, septembre 2015 (à la demande d'Intel Security)
2. Rapport de Gartner, *Market Guide for Cloud Access Security Brokers* (Guide du marché des intermédiaires de sécurité de l'accès au cloud), Craig Lawson, Neil MacDonald et Brian Lowans, 22 octobre 2015

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com