

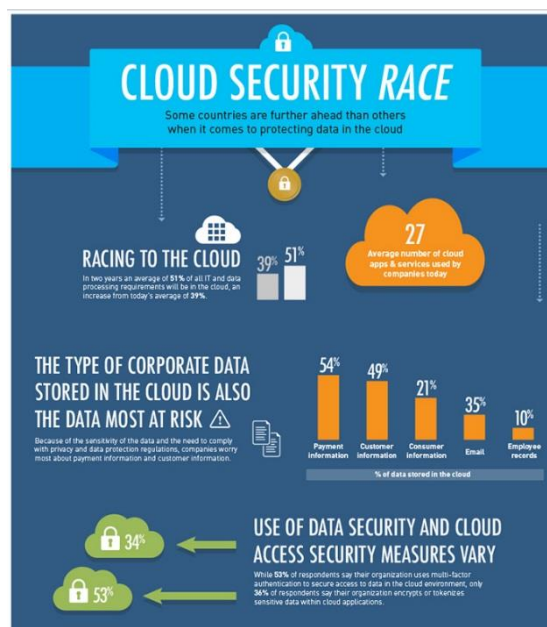
pressrelease

Étude de Gemalto et Ponemon Institute : on observe de gros écarts entre les pays au niveau des attitudes en ce qui concerne la protection des données dans le cloud

- L'étude révèle des disparités régionales dans l'adoption de la sécurité dans le cloud : les entreprises allemandes sont quasiment deux fois plus susceptibles de sécuriser leurs informations confidentielles ou sensibles dans le cloud (61 %) que leurs homologues britanniques (35 %), brésiliennes (34 %) et japonaises (31 %)
- La moitié des entreprises mondiales sont convaincues que les informations de paiements (54 %) et les données clients (49 %) courent un risque dans le cloud
- Plus de la moitié (57 %) pense que l'utilisation du cloud accroît le risque de conformité

Amsterdam, le 16 janvier 2018 – Gemalto, le leader mondial de la sécurité numérique, peut aujourd'hui révéler qu'alors que la grande majorité des sociétés internationales (95 %) fait appel à des services dans le cloud¹, on relève un fossé immense au niveau des mesures de sécurité adoptées par ces entreprises sur les différents marchés. Les entreprises reconnaissent en moyenne que seuls deux cinquièmes (40 %) des données stockées dans le cloud sont sécurisées à l'aide de solutions de chiffrement et de gestion par clé.

Les conclusions – qui font partie de la « [2018 Global Cloud Data Security Study](#) », l'édition 2018 de l'étude sur la sécurité des données dans le cloud conduite par Ponemon Institute sur demande de Gemalto – révèlent que les entreprises au Royaume-Uni (35 %), au Brésil (34 %) et au Japon (31 %) sont moins prudentes que leurs homologues allemandes (61 %) lorsqu'elles partagent des informations sensibles et confidentielles stockées dans le cloud avec des tiers. Plus de 3 200 informaticiens et acteurs de la sécurité informatique dans le monde entier ont été interrogés dans le cadre de l'étude afin de mieux comprendre les grandes tendances sur les pratiques de gouvernance et de sécurité des données pour les services basés dans le cloud.



La longueur d'avance de l'Allemagne en matière de [sécurité dans le cloud](#) concerne sa mise en application de mesures de contrôle tels que le chiffrement et la tokenisation. La majorité (61 %) des entreprises allemandes ont déclaré qu'elles sécurisent leurs informations sensibles ou confidentielles

¹ <https://www.rightscale.com/lp/2017-state-of-the-cloud-report?campaign=7017000000vFyc>

lorsque celles-ci sont stockées dans l'environnement du cloud, devant les entreprises américaines (51 %) et japonaises (50 %). Le niveau de sécurité appliqué augmente encore plus lors de l'envoi et de la réception de données par l'entreprise, pour s'élever à 67 % pour l'Allemagne, suivie par le Japon (62 %) et l'Inde (61 %).

Fait décisif, toutefois, plus des trois quarts (77 %) des entreprises à travers le monde reconnaissent l'importance d'avoir la capacité de mettre en œuvre des solutions cryptologiques, telles que le chiffrement. Cela devrait encore s'intensifier, neuf entreprises sur dix (91 %) estimant que cette aptitude gagnera en importance au cours des deux prochaines années – en hausse par rapport au chiffre de 86 % enregistré l'an dernier.

Gestion de la vie privée et de la réglementation dans le cloud

Malgré l'adoption croissante de l'informatique dans le cloud et les bénéfices qui vont avec, il semble que les entreprises internationales soient encore méfiantes. Plus inquiétant, la moitié d'entre elles déclare que les informations de paiement (54 %) et les données client (49 %) courent un risque lorsqu'elles sont stockées dans le cloud. Plus de la moitié (57 %) des entreprises internationales pense que l'utilisation du cloud les met davantage en position d'enfreindre les règles sur la protection de la vie privée et des données, soit un léger recul par rapport au chiffre de 62 % recueilli en 2016.

En raison de ce risque perçu, la quasi-totalité (88 %) pense que le nouveau Règlement général sur la protection des données (RGPD) exigera des changements au niveau de la gouvernance dans le cloud, deux entreprises interrogées sur cinq (37 %) déclarant même que le RGPD devrait imposer des changements majeurs. Outre la difficulté de satisfaire aux obligations réglementaires, trois quarts des personnes interrogées dans le monde (75 %) ont également déclaré qu'il est plus complexe de gérer les règlements sur la protection de la vie privée et des données dans l'environnement du cloud que sur les réseaux au sein de l'entreprise, la France (97 %) et les États-Unis (87 %) évoquant la plus grande complexité, devançant de peu l'Inde (83 %).

La tête dans les nuages

Malgré la prédominance de l'usage du cloud, l'étude a montré l'existence d'un fossé dans la connaissance, au sein des entreprises, des services qui sont utilisés. Seul un quart (25 %) des informaticiens et des acteurs de la sécurité informatique a indiqué être très confiant dans leur connaissance de tous les services dans le cloud que leur entreprise utilise, un tiers se déclarant seulement confiant (31 %) dans sa connaissance de ces services.

À y regarder de plus près, l'informatique cachée (ou *shadow IT*) pourrait continuer à poser des difficultés. Plus de la moitié des entreprises australiennes (61 %), brésiliennes (59 %) et britanniques (56 %) n'a pas la certitude de connaître toutes les applications informatiques, plateformes ou services d'infrastructures dans le cloud utilisés par leur entreprise. Le niveau de confiance est plus élevé ailleurs, puisque seul environ un quart des personnes interrogées en Allemagne (27 %), au Japon (27 %) et France (25 %) ne se déclare pas confiant à cet égard.

Heureusement, la grande majorité (81 %) estime que la capacité d'utiliser des techniques d'authentification forte pour accéder aux données et aux applications dans le cloud est essentielle ou très importante. Les entreprises australiennes sont les plus motivées par la mise en place de mesures

d'authentification, 92 % convenant que cela permettrait de s'assurer que seules les personnes autorisées pourraient avoir accès à certaines données et applications dans le cloud, devant l'Inde (85 %) et le Japon (84 %).

« Même s'il est satisfaisant de constater que des pays comme l'Allemagne prennent la question de la sécurité dans le cloud au sérieux, on observe des attitudes inquiétantes dans le reste du monde », commente Jason Hart, Directeur technologique en charge de la protection des données de Gemalto. « Cela va peut-être jusqu'à la moitié des entreprises qui jugent que le cloud rend plus difficile la protection des données, alors que c'est l'inverse qui est vrai.

« L'avantage du cloud tient à sa commodité, à son évolutivité et à la maîtrise des coûts, en offrant des options aux entreprises auxquelles elles ne pourraient pas avoir accès ni se permettre financièrement seules, en particulier en matière de sécurité. Toutefois, si la sécurisation des données est plus facile, il convient de ne jamais partir du postulat que l'adoption du cloud rime automatiquement avec protection de l'information. Il suffit de prendre les infractions récentes d'Accenture et d'Uber comme autant d'exemples de données dans le cloud qui se sont retrouvées exposées. Peu importe où se trouvent les données, des mesures de contrôle appropriées telles que le chiffrement et la tokenisation doivent être positionnées à la source des données. Une fois en place, tous les problèmes de conformité devraient être résolus. »

Méthodologie de recherche

Cette recherche a été conduite par le [Ponemon Institute](#) au nom de Gemalto auprès de 3 285 informaticiens et acteurs de la sécurité informatique qui ont été interrogés aux États-Unis (575), au Royaume-Uni (405), en Australie (244), en Allemagne (492), en France (293), au Japon (424), en Inde (497) et au Brésil (355).

Ressources

- Consulter le [site de l'édition 2018 de l'étude sur la sécurité des données mondiales dans le cloud](#) pour explorer les différences entre les régions plus en détail ou télécharger le rapport
- Rejoindre Gemalto et le Ponemon Institute pour un séminaire en ligne consacré aux « Grandes tendances de la sécurité du cloud » le 27 février prochain – cliquer ici pour s'inscrire.
- En savoir plus sur [solutions pour la sécurité des données dans le cloud](#) de Gemalto
- En savoir plus sur la recherche de Gemalto sur la sécurité des données.

À propos de Gemalto

Gemalto (Euronext NL0000400653 GTO) est le leader mondial de la [sécurité numérique](#), avec un chiffre d'affaires 2016 de 3,1 milliards d'euros et des clients dans plus de 180 pays. Nous apportons la confiance dans un monde de plus en plus interconnecté.

Des logiciels sécurisés à la biométrie et au chiffrement, nos technologies et services permettent aux entreprises et aux gouvernements d'authentifier les identités mais également de protéger les données

afin qu'elles restent en sécurité et assurent des services dans les appareils personnels, les objets connectés, le cloud et sur les réseaux.

Les solutions de Gemalto sont au cœur de la vie moderne, du paiement à la sécurité de l'entreprise en passant par l'internet des objets. Nous authentifions les personnes, les transactions ainsi que les objets, chiffons les données et créons de la valeur pour les logiciels – permettant ainsi à nos clients d'offrir des services numériques sécurisés à des milliards de personnes et d'objets.

Présent dans 48 pays, Gemalto emploie plus de 15 000 personnes travaillant depuis 112 bureaux, 43 centres de personnalisation et de données et 30 pôles de Recherche et de Développement logiciel.

Pour plus d'informations, visitez notre site www.gemalto.com/france, ou suivez [@GemaltoFrance](https://twitter.com/GemaltoFrance) sur twitter.

Relations presse de Gemalto :

Tauri Cox
Amérique du Nord
+1 512 257 3916
tauri.cox@gemalto.com

Sophie Dombres
Europe, Moyen-Orient et Afrique
+33 4 42 55 36 57 38
sophie.dombres@gemalto.com

Jaslin Huang
Asie-Pacifique
+65 6317 3005
jaslin.huang@gemalto.com

Enriqueta Sedano
Amérique latine
+52 5521221422
enriqueta.sedano@gemalto.com

Le texte de ce communiqué, issu d'une traduction, ne doit en aucune manière être considéré comme officiel. La seule version du communiqué qui fasse foi est celle du communiqué dans sa langue d'origine, l'anglais, qui prévaut donc en cas de divergence avec la traduction.