Deloitte.

Dissipez vos soucis infonuagiques

Réduire les risques de votre transition vers l'infonuagique

Table des matières

1 Introduction

2 Deux importants

3 Gouvernance et responsabilité

4 Élaborer une stratégie de sécurité infonuagique

5 Concentrer vos efforts sur la gestion des identités et des accès

Introduction

Les organisations de tous les secteurs mettent continuellement tout en œuvre pour évoluer de manière à devenir plus agiles et à avoir la capacité de s'adapter rapidement. Elles cherchent des moyens de réduire les frictions, de favoriser l'innovation, d'offrir une meilleure expérience de service à la clientèle et de demeurer concurrentielles dans un contexte de plus en plus difficile.

L'adoption de l'infonuagique est souvent au cœur de cette transformation, puisqu'elle procure un environnement souple qui permet à l'organisation de satisfaire ces besoins. Les services d'infonuagique sont habituellement faciles d'accès et ils sont pratiques à utiliser, mais ils peuvent aussi engendrer des risques importants pour les organisations qui n'ont pas la capacité de s'adapter au nouveau modèle.

Cependant, les organisations ne sont bien souvent pas conscientes des grandes différences qui existent entre la création et la gestion d'une infrastructure technologique dans le nuage et la gestion d'une infrastructure sur place.

Deux importants

Les perspectives traditionnelles peuvent engendrer une plus grande vulnérabilité

Les équipes responsables de la technologie abordent parfois l'infonuagique avec une perspective traditionnelle. Au lieu de prendre le temps de comprendre les particularités propres à des services d'infonuagique donnés et d'évaluer comment les intégrer à de nouvelles pratiques d'affaires, les équipes des TI peuvent s'efforcer de reproduire les processus traditionnels dans le contexte de l'infonuagique et de simplement déplacer les données existantes dans le nuage, tentant ainsi de faire passer le système d'un environnement à un autre, sans avoir effectué les adaptations qui s'imposaient. Par exemple, au lieu d'utiliser le dispositif d'ouverture de session faisant partie de l'infonuagique, on pourrait tenter de virtualiser celui qui existait déjà depuis des années dans le système de TI sur place, alors que les fonctions par défaut des services d'infonuagique sont plus simples, plus rapides et probablement supérieures.

Les processus, pratiques ou systèmes traditionnels reproduits ne sont pas toujours bien configurés pour être intégrés à l'infonuagique, contrairement à ceux optimisés faisant partie intégrante du nuage. La mauvaise configuration peut être à l'origine de nouveaux risques qui rendent une entreprise et ses données vulnérables.

En 2019, des incidents liés à la sécurité ont fait ressortir que cette vulnérabilité ouvre la porte à des abus. Les nouvelles prévisions montrent que l'on s'attend à ce que plus de 99 %[1] des cyberattaques infonuagiques soient liées à une mauvaise configuration. Même si de plus en plus d'organisations adoptent l'infonuagique, elles ont encore tendance à simplement transposer dans le nuage les mécanismes de sécurité utilisés pour les infrastructures sur place, qui n'ont pas été conçues pour bien fonctionner avec les services d'infonuagique.

Les lacunes dans les configurations de sécurité exposent d'anciens points faibles

Les organisations ont voulu protéger leurs données contre les nouvelles menaces et attaques, mais même si elles font un meilleur usage des nouvelles technologies pour protéger leur environnement, les cyberattaques continuent d'exploiter leurs anciens points faibles. La modélisation des menaces, les tests de pénétration et les évaluations de la vulnérabilité spécifiques aux plateformes infonuagiques peuvent aider votre organisation à mieux comprendre comment les menaces ont évolué.

Dans bien des cas, les ressources sont mal configurées parce que l'équipe chargée de l'implantation ou de la mise en œuvre soit n'a pas les connaissances nécessaires, soit elle applique des processus traditionnels qui ne conviennent pas à un environnement d'infonuagique. Par exemple, la configuration de l'acheminement réseau au moyen du chemin existant du fournisseur de services d'infonuagique doit être effectuée correctement pour bien gérer le cheminement des données. L'un des meilleurs moyens pour les organisations d'atténuer ce risque consiste à utiliser des systèmes de gestion de posture de sécurité infonuagique et des outils natifs de surveillance de la conformité de l'infonuagique fondés sur les meilleures pratiques de sécurité.

Si les lacunes relatives à la sécurité d'une configuration ne sont pas décelées, les faiblesses existantes risquent d'être exploitées. Il est donc impératif d'avoir une bonne visibilité des charges de travail dans l'environnement et de mettre en œuvre des contrôles appropriés en utilisant des points de référence (par la gestion automatisée de la configuration et la correction des faiblesses relevées dans la configuration). Le personnel doit être en mesure de gérer et de configurer les outils propres à l'infonuagique en fonction de ces points de référence définis.

1. Innovation Insight for Cloud Security Posture Management (en anglais seulement) Gartner, publié le 25 janvier 2019 – ID G00377795

Dissipez vos soucis infonuagiques | Réduire les risques de votre transition vers l'infonuagique

Réduire le risque : par où commencer

- **Comprendre ce que l'on fait déjà dans le nuage.** Évaluer comment votre organisation utilise déjà le nuage. Déterminer les risques qui y sont associés ainsi que les moyens pris pour gérer et atténuer ces risques. Déterminer quelles balises existent, le cas échéant, pour l'utilisation de l'infonuagique.
- **Effectuer une analyse comparative de l'utilisation de l'infonuagique.** Afin de comprendre les lacunes et les risques associés à l'infonuagique, il faut comparer comment vous vous servez du nuage par rapport aux cadres bien établis représentant les meilleures pratiques pour l'architecture d'infonuagique, comme ceux définis par le National Institute of Standards and Technology (NIST) et le Center for Internet Security (CIS) des États-Unis. Cette évaluation permet de déterminer ce que l'organisation fait bien et ce qu'elle doit améliorer pour atténuer les risques liés à l'infonuagique.
- **Élaborer une stratégie de gestion de l'infonuagique.** Veiller à ce que l'organisation se dote d'une stratégie d'infonuagique claire bien diffusée qui indique le but de l'infonuagique et comment la stratégie contribue à l'atteinte de ce but. L'élaboration de la stratégie, qui peut évoluer comme l'utilisation de l'infonuagique, amènera les différentes parties à travailler de concert et aidera à réduire au minimum les expérimentations improvisées en infonuagique.
- **Rehausser la gestion en intégrant l'infonuagique.** Le modèle de gestion des TI de l'organisation doit être revu en fonction des particularités découlant du fait que l'entreprise utilise l'infonuagique pour exercer ses activités. Il faut établir des responsabilités claires pour les initiatives d'infonuagique ainsi que des règles d'engagement pour diriger l'utilisation de l'infonuagique et la gestion des données qui sont dans le nuage. On doit mettre en place des mécanismes capables de détecter les problèmes dans les activités liées à l'infonuagique et les régler rapidement et efficacement.
- **Investir dans la formation sur l'infonuagique.** L'infonuagique est encore quelque chose de nouveau pour la plupart des organisations, et le niveau de compréhension de son utilité pour l'entreprise varie grandement. Il faut veiller à donner aux dirigeants et aux membres de leur équipe une formation continue appropriée de manière à ce qu'ils possèdent les connaissances nécessaires sur l'infonuagique.

Gouvernance et responsabilité

S'il est aussi difficile pour les entreprises de comprendre et de gérer les risques de l'infonuagique, c'est que rares sont celles qui ont une vision claire de leur stratégie relative à l'infonuagique et des risques qui y sont associés.

D'après notre expérience, le chef de la direction, le chef de l'information, le chef des données et les autres dirigeants ont souvent une vision divergente de la stratégie et des résultats. En fait, la plupart des entreprises n'ont pas de stratégie globale d'infonuagique. À la place, elles ont une série d'initiatives tactiques lancées pour différentes raisons en vue d'innover et de parvenir à un degré de compétitivité supérieur. Il est donc difficile pour les entreprises de gérer efficacement l'infonuagique et d'atténuer les risques que représente pour elles la transition vers le nuage. Mais difficile ne veut pas dire impossible.

1. Préparer la gouvernance des TI à la transition vers l'infonuagique

Une bonne gouvernance des services d'infonuagique est un aspect clé pour réduire les risques des programmes d'infonuagique. C'est d'autant plus vrai que l'adoption des services d'infonuagique peut être très facile, rapide et peu coûteuse. Le plus souvent, il suffit d'avoir une personne qui peut utiliser une carte de crédit pour pouvoir enregistrer rapidement dans le nuage les données de l'entreprise, comme les coordonnées des clients. En quelques minutes à peine, une entreprise peut envoyer par mégarde toutes ses données dans le nuage. D'où l'importance de bien faire connaître les services d'infonuagique aux responsables des TI et de la sécurité des données dans l'organisation. En connaissant les services qu'utilise votre entreprise, vos équipes pourront bien se préparer à se protéger elles-mêmes et à protéger les données dans le nuage.

Afin d'éviter les difficultés réglementaires, l'organisation doit veiller à avoir les moyens de contrôler et de gérer quelles données sont enregistrées dans le nuage, leur emplacement, la manière dont leur sécurité est assurée et le moment où elles sont effacées. L'inclusion de l'infonuagique dans la politique de classification de l'information et l'utilisation d'étiquettes pour les ressources infonuagiques permettent d'obtenir une telle visibilité. Par exemple, le téléchargement de données sur des citoyens de l'Union européenne peut faire en sorte qu'une entreprise soit soudainement tenue de se conformer au règlement général sur la protection des données de l'Union européenne.

Enfin, l'organisation doit voir à ne pas laisser traîner de grandes quantités d'« anciennes » données de crainte de les y oublier, jusqu'à ce qu'un pirate ou un cybercriminel les découvre. Comme on l'a observé à maintes reprises ces dernières années, les atteintes à la sécurité des données peuvent avoir de graves répercussions sur les plans des finances, de la réputation, de la réglementation et du droit, et il faut souvent beaucoup de temps pour s'en remettre.

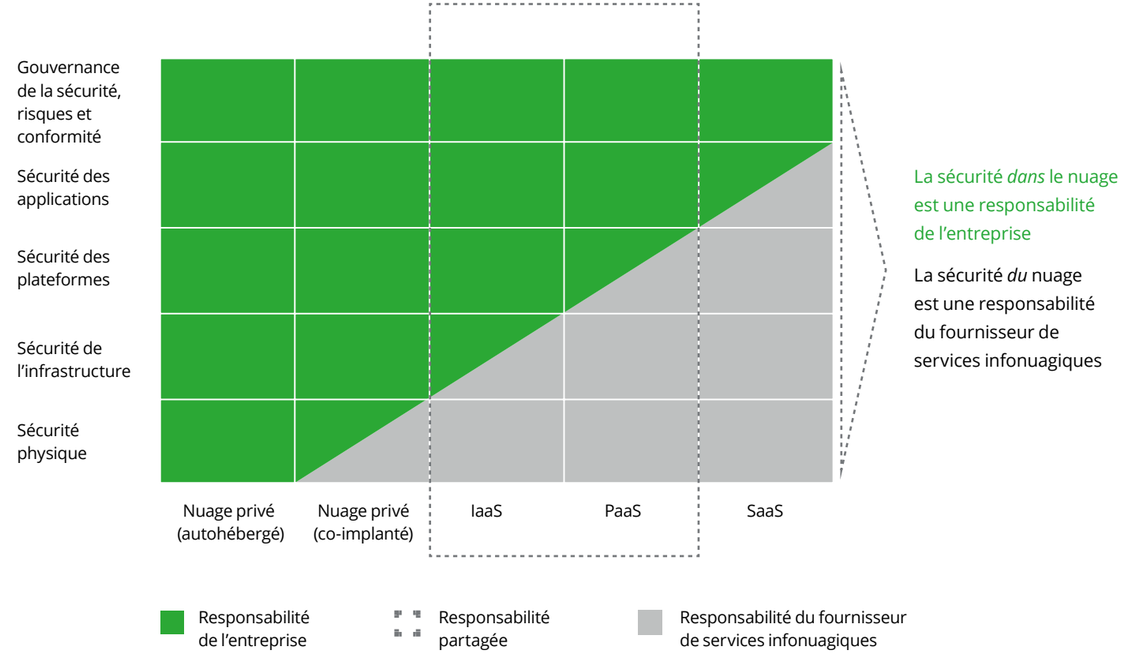
Dissipez vos soucis infonuagiques | Réduire les risques de votre transition vers l'infonuagique

2. Promouvoir le modèle de responsabilité partagée

Des organisations ont la vague impression que l'adoption de l'infonuagique réduira les efforts nécessaires pour assurer la gestion et la sécurité des ressources, qu'elles fassent la migration complète à l'infonuagique ou qu'elles utilisent une combinaison de systèmes sur place et d'infonuagique. À l'opposé, d'autres organisations croient que la protection des données dans le nuage relève toujours de leur responsabilité, peu importe le modèle de services qu'elles utilisent.

Dans les faits, la sécurité des données dans le nuage est une responsabilité partagée entre le client et le fournisseur de services, et la part de responsabilité de l'organisation dépend du modèle de services choisi.

En général, les modèles d'infrastructure-service (IaaS) attribuent une plus grande part de responsabilité de sécurité au client, tandis que dans les modèles de plateforme-service (PaaS) et de logiciel-service (SaaS), la plus grande part de responsabilité appartient au fournisseur de services d'infonuagique. Il importe néanmoins d'aller plus dans le détail pour dissiper toute confusion avec le fournisseur dès le départ. Après l'avoir clairement défini, n'hésitez pas à faire la promotion de votre modèle de responsabilité partagée avec vos équipes chargées des TI et de la sécurité. Plus il y aura de personnes au courant des responsabilités de chacun, mieux votre organisation sera préparée.



Élaborer une stratégie de sécurité infonuagique

Pour élaborer une stratégie destinée à protéger vos renseignements dans le nuage, vous devez d'abord **comprendre les nouveaux risques** auxquels votre organisation s'expose. Il importe d'établir l'ordre de priorité des risques pertinents pour votre environnement de nuage public en fonction des divers règlements qui pourraient s'appliquer, ainsi que le niveau de sensibilité des données de l'entreprise que vous songez à faire passer dans le nuage.

Déterminez quels sont vos renseignements les plus précieux, puis **définissez les risques** afin de comprendre comment ces renseignements peuvent être menacés et protégés. Quels renseignements précis sont exposés à un risque dans chacun des scénarios infonuagiques? En quoi consistent les vulnérabilités et les menaces potentielles? Quelle est l'importance des renseignements à risque?

Dans la mesure où les bonnes précautions sont prises, les environnements infonuagiques peuvent être aussi sûrs que les environnements sur place. Mais tout comme dans le cas de la sécurité physique, plus vous prenez des mesures de sécurité infonuagique, plus elles seront complexes et coûteuses. Vous pouvez effectuer une **évaluation de la menace des risques infonuagiques et des exercices de modélisation des menaces infonuagiques** adaptés à votre environnement ou à vos applications infonuagiques proposés ou existants. En déterminant quels sont les risques et en établissant votre tolérance aux risques, vous serez en mesure de prendre des décisions plus éclairées quant à votre utilisation de l'infonuagique. Cela vous permettra d'adapter vos mesures de sécurité et votre budget à l'environnement afin d'assurer l'utilisation la plus efficace possible de vos ressources.

Ensuite, **mettez de l'ordre dans votre environnement.** Quels changements devraient être apportés à vos modèles opérationnels et organisationnels pour éviter que le nuage soit exploité en vase clos ou sous forme de système parallèle non géré? Cela signifie qu'il faut établir de nouvelles priorités infonuagiques dans la matrice RACI (Responsable, Imputable, Consulté, Informé), en veillant à ce que les **normes et contrôles de cybersécurité infonuagique** s'insèrent dans le cadre de cybersécurité que vous avez choisi (p. ex., NIST, ISO, CSA) et permettent aux environnements infonuagiques de s'intégrer entièrement à vos services de cybersécurité existants.

Cela n'arrivera pas du jour au lendemain et **nécessitera la mise en place de personnel.** Les spécialistes en cybersécurité infonuagique sont rares et coûtent cher. Votre équipe de cybersécurité actuelle ne saura pas comment traiter les incidents de sécurité infonuagique ou les stratégies de résolution, et votre équipe infonuagique est susceptible de ne pas saisir toute l'ampleur de la cybersécurité d'entreprise. Créez d'abord des équipes souples et intégrées, réunissant les meilleurs acteurs des deux univers, et assurez leur formation croisée.

Ces équipes auront besoin d'assistance; aussi, l'automatisation et la surveillance s'imposent. C'est le bon moment pour réfléchir à une approche de type **SaC (la sécurité en tant que code).** Les pratiques de développement opérationnel de la sécurité et la surveillance automatisée seront des éléments distinctifs pour les organisations qui souhaitent miser sur la vitesse promise par le nuage, mais qui a été énormément ralentie par les préoccupations à l'égard de la sécurité. En investissant dans des outils tels que la gestion des informations et des événements de sécurité **(SIEM)** propres à l'infonuagique ou prêts pour le nuage et la **gestion de la situation de sécurité infonuagique,** vous serez davantage en mesure de prendre la sécurité en main. Des fichiers de configuration de la sécurité comme Azure Policy, AWS Organizations et les modèles AWS CloudFormation peuvent être adaptés aux besoins de votre entreprise et déployés à grande échelle à l'aide de pipelines modernes de gestion des identités et des accès (intégration continue et exécution continue). Et surtout, ces outils peuvent tous être configurés de façon à refléter la politique de cybersécurité que vous avez choisie, ce qui donne à ces équipes la chance de bien s'en tirer.

Dissipez vos soucis infonuagiques | Réduire les risques de votre transition vers l'infonuagique

Concentrer vos efforts sur la gestion des identités et des accès

L'un des aspects les plus importants de la sécurité infonuagique est la gestion des identités et des accès (GIA). Le fait que les périmètres réseau sont éliminés ou s'estompent dans le nuage entraîne de nouvelles difficultés lorsqu'il s'agit de réagir aux risques, notamment comment administrer correctement les contrôles d'accès granulaires aux services infonuagiques. Chacune des entités et des ressources infonuagiques comporte une identité qui doit être sécurisée.

Voici des capacités et des considérations essentielles associées à la gestion des identités dans le nuage :

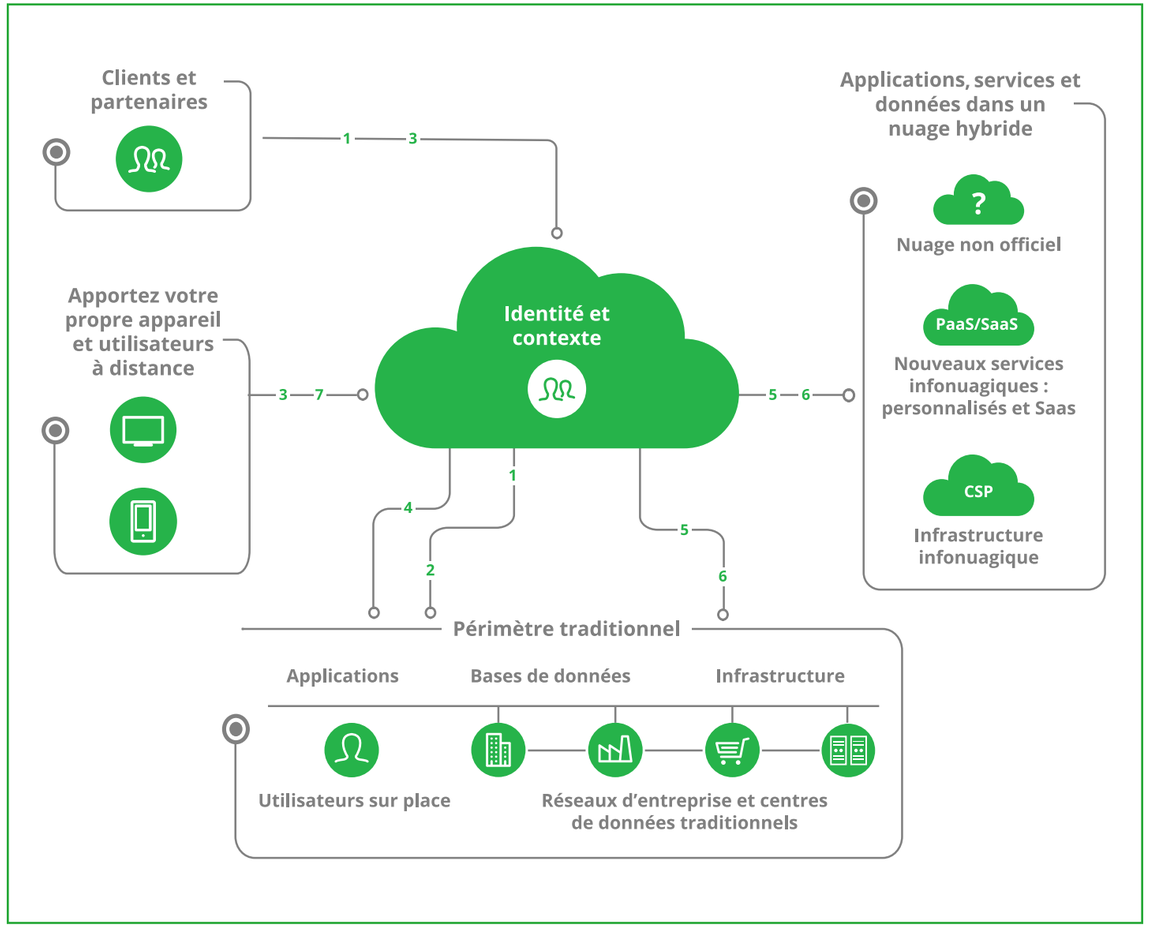
- Les gens constituent le nouveau périmètre – consacrez autant de temps à la protection des gens au sein des environnements infonuagiques qu'à la mise en place de la sécurité des réseaux infonuagiques.
- L'infonuagique en entreprise nécessite une intégration et des identités fédérées, s'appuyant sur des annuaires d'entreprise;
- L'authentification unique et l'authentification multifacteur d'entreprise fondées sur une stratégie d'accès conditionnel doivent être activées pour tous les utilisateurs;
- L'attribution d'utilisateurs du nuage, les rôles de GIA et le contrôle d'accès en fonction des rôles nécessitent une planification et une conception minutieuses, mais peuvent approfondir la sécurité;
- La gestion des comptes privilégiés et la gestion des identités privilégiées peuvent faire appel à des solutions qui sont propres au nuage ou prêtes pour le nuage;
- La gestion des applications et données mobiles est importante lorsque le nuage s'étend aux utilisateurs d'appareils mobiles.

Voici certains des plus importants schémas de GIA :

- L'intégration des solutions de gestion des identités infonuagiques dès le départ. Même si de nombreuses entreprises n'hésitent pas à créer des mesures de sécurité en vase clos qui utilisent des approches et des technologies différentes, avec le temps, une telle stratégie peut devenir contre-productive. Tôt ou tard, vous devrez opter pour un modèle de sécurité unique.
- Les solutions de GIA actuellement disponibles sur le marché sont axées soit sur l'infonuagique, soit sur l'entreprise. Concentrez-vous sur la conception et l'architecture de votre solution de sécurité fondée sur les identités, puis sélectionnez la technologie. Même si la solution est plus complexe, l'architecture devrait s'avérer durable au fil des changements technologiques. Ne laissez jamais la technologie dicter les exigences ou la conception.
- Ne lésinez pas sur les essais, y compris les tests de sécurité de type chapeau blanc. Ceux-ci pourraient vous amener à comprendre où se situent les vulnérabilités au sein de votre système et, par conséquent, de faire un meilleur choix concernant les approches et l'utilisation des technologies de sécurité. Les systèmes de gestion des identités et de l'accès axés sur l'infonuagique sont de plus en plus nécessaires à mesure que l'« identité » infonuagique se définit. L'identité n'est plus seulement humaine, mais peut représenter des secrets, des conteneurs et des dispositifs de l'Internet des objets parmi une multitude de possibilités[2]. Cependant, cela pourrait être attribuable au fait que les systèmes d'entreprise sur place sont beaucoup moins sécurisés et sont donc des cibles plus faciles.
- Au moment de la conception, assurez-vous de prendre en compte des aspects comme la performance. Tandis que la plupart des systèmes de GIA ne provoquent pas de ralentissement, c'est un phénomène qui n'est pas impossible et qui sera difficile à corriger après le déploiement. Ceux-ci peuvent entraîner des problèmes au sein des systèmes de sécurité, car les utilisateurs trouvent vite des moyens de contourner la sécurité.
- Assurez-vous de prendre en compte votre secteur et les règlements que vous devez respecter. Ceux-ci sont normalement gérés à l'aide du système de gouvernance des identités au sein du GIA et doivent être compris dès le départ. Il est difficile de modifier ces politiques après la mise en œuvre.

2. 2021 Planning Guide for Identity and Access Management (en anglais seulement) Gartner, publié le 9 octobre 2020 – ID G00729005

Dissipez vos soucis infonuagiques | Réduire les risques de votre transition vers l'infonuagique



La gestion des comptes privilégiés et la gestion des identités privilégiées peuvent faire appel à des solutions qui sont propres au nuage ou prêtes pour le nuage.

Gérer les risques de l'infonuagique, et exploiter son plein potentiel

L'infonuagique aidera grandement les entreprises à accroître leur rapidité, leur agilité et leur compétitivité dans les années à venir, peu importe leur secteur d'activité. Il est néanmoins impératif de gérer, de réduire et d'atténuer les risques liés à l'infonuagique afin d'assurer la viabilité et la force de l'entreprise à long terme. Le moment est venu pour votre organisation de miser sur tout ce que l'infonuagique a à offrir tout en tenant compte des risques.

Personne-ressource

Rob Masse
Associé,
Conseils en gestion des risques
rmasse@deloitte.ca

Remerciements

Aaron Fleming
Directeur de service,
Conseils en gestion des risques

Ian Guthrie
Directeur principal,
Conseils en gestion des risques

Rene Heroux
Directeur principal,
Consultation

Naresh Kurada
Directrice de service,
Conseils en gestion des risques

Grégory Lemaire
Directeur principal,
Conseils en gestion des risques

Kevin Young
Associé, Consultation

Deloitte.

www.deloitte.ca

À propos de Deloitte
Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans différents secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500[MD] par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.

Pour en apprendre davantage sur les quelque 312 000 professionnels de Deloitte, dont plus de 12 000 font partie du cabinet canadien, veuillez nous suivre sur LinkedIn, Twitter, Instagram ou Facebook.

Conçu et produit par L'Agence| Deloitte Canada. 20-3190014