WHITE PAPER

Extension du contrôle d'accès au cloud

Les entreprises sont de plus en plus nombreuses à utiliser des applications SaaS (Software-as-a-Service). Même si elles présentent des avantages considérables, ces applications peuvent également entraîner des failles au niveau des accès non autorisés. En raison de la popularité croissante de ces applications, il s'avère essentiel de se doter d'une solution abordable et facilement gérable qui permette de superviser et de contrôler l'accès des utilisateurs aux informations hébergées en mode SaaS. La sécurité, la création de rapports de conformité et la facilité d'accès figurent parmi les principaux défis auxquels sont confrontées les entreprises, et celles-ci se doivent de les gérer efficacement. Si la complexité en matière de sécurité des accès autorisés n'est pas prise en compte par les entreprises, elles opteront pour une solution incomplète, non sécurisée et nécessitant une intervention manuelle.

NetIQ

NetIQ | WHITE PAPER

Table des matières

Les solutions SaaS : un atout pour les entreprises

L'informatique en nuage (cloud computing) fait apparaître un nouveau paradigme sur le marché. Tandis que les budgets informatiques sont gelés, les BU (Business Units) deviennent des facteurs budgétaires déterminants. Souvent, les entreprises diffèrent leurs dépenses d'investissement, ce qui a pour effet de retarder l'adoption de nouveaux modèles commerciaux qui permettraient aux BU et au service informatique d'optimiser leur efficacité. De ce fait, les entreprises privilégient de plus en plus le modèle SaaS (Software-as-a-Service) pour l'utilisation des applications.

L'utilisation d'applications SaaS permet d'éviter les frais initiaux généralement associés aux nouveaux déploiements. Elle offre également une rapidité d'évolution sans commune mesure avec celle des applications traditionnelles. Par ailleurs, le SaaS offre trois avantages principaux par rapport à l'achat conventionnel de logiciels :

- Les applications SaaS sont hébergées dans le cloud et accessibles en tout lieu.
- L'accès mobile est immédiatement disponible.
- Le service informatique est dispensé de gérer des projets de mise à jour visant à obtenir les derniers correctifs ou fonctionnalités, car les applications sont mises à jour en permanence.

Face à tous ces avantages manifestes, il n'est pas surprenant que le marché des solutions SaaS évolue à un rythme effréné. En 2011, ce marché a atteint 21,2 milliards de dollars et d'après certaines estimations, il pourrait représenter 132,5 milliards de dollars d'ici 2020[1]. Gartner prévoit les plus forts taux de croissance d'ici 2016[2].

Les risques de l'informatique en nuage

Les utilisateurs professionnels qui adoptent avec enthousiasme des applications SaaS introduisent également de nouveaux risques pour leur entreprise. En matière d'applications SaaS, parmi les dix principales préoccupations des services informatiques, les trois premières concernent la sécurité[3].

Outre les risques juridiques et financiers, les violations de sécurité s'accompagnent d'une publicité négative dont la gestion peut s'avérer cauchemardesque. Ces gros titres ne vous rappellent-ils rien ?

- « Violation de la sécurité des cartes de crédit Citi identifiée », CNNMoney, 9 juin 2011
- « Google révèle une violation de la sécurité des données de Gmail », Cryptzone, 2 juin 2011
- « Sony gèle 93 000 comptes en ligne suite à une violation de sécurité », Forbes, 12 octobre 2011
- « Le FMI victime d'une cyberattaque de grande ampleur », BBC, 12 juin 2011
- « Une violation de sécurité dévastatrice expose des données militaires », eSecurityPlanet.com, août 2010
- « Violation de sécurité chez Lockheed Martin », Wall Street Journal, 27 mai 2011
- « La réputation de LinkedIn entachée après une violation de sécurité », Calgary Herald, 9 juin 2012

1 Forrester Research Inc. 2011
2 Gartner Forecast : Public Cloud Services, Worldwide and Regions, Industry Sectors, 2010-2015, mise à jour 2011
3 The Aberdeen Group, 2011

La sécurité des données sensibles et de la propriété intellectuelle est essentielle pour toute entreprise. Plans et stratégies marketing, secrets concernant les gammes de produits, informations relatives aux clients : les entreprises doivent accéder quotidiennement à leurs données tout en les protégeant de leurs concurrents et des cyberattaques.

Vos informations sont-elles réglementées ? Si vous travaillez dans un secteur réglementé, notamment la finance, les assurances, l'énergie ou la santé, vous devez pouvoir prouver la conformité de votre entreprise à des directives spécifiques qui régissent le contrôle de l'accès aux informations. Une fois que le service informatique maîtrise ces exigences pour vos applications sur site, un niveau similaire de contrôle est requis pour les applications en nuage. Sur site, votre structure informatique intègre des processus qui assurent un accès aux seules personnes autorisées et la possibilité de surveiller cet accès. Pour maintenir la conformité, le service informatique doit étendre ces contrôles et fonctions de création de rapports de façon à inclure les informations de l'entreprise qui se trouvent dans le cloud. Les infrastructures distinctes, externes aux processus existants, n'offrent pas la fiabilité et l'efficacité requises.

Votre contrôle s'étend-il au-delà des limites de votre entreprise ? Il peut être difficile de mesurer l'utilisation des applications SaaS. L'utilisation de ces applications par les services et secteurs d'activités résulte souvent d'une série de décisions tactiques qui évoluent avec le temps plutôt que de consignes émises par la direction. Par ailleurs, lorsque l'utilisation des applications SaaS est un choix tactique, les utilisateurs professionnels impliquent rarement le service informatique : c'est l'administrateur commercial qui est le plus souvent désigné pour maintenir les comptes à jour. Il s'agit d'une approche ponctuelle et manuelle. L'intégration des nouveaux employés peut perturber l'accès aux applications. De plus, lorsque des employés changent de rôle ou quittent l'entreprise, tout manquement en termes de déprovisioning laisse la porte ouverte à des utilisations malveillantes de leur part. La question est la suivante : qui est responsable de la sécurisation de l'accès ? Est-ce que la sécurité et la conformité des accès relèvent de la responsabilité du service informatique ? Êtes-vous certain qu'aucun utilisateur malveillant n'a accès aux informations confidentielles de votre entreprise dans le cloud ?

La plupart des entreprises utilisent Active Directory comme espace de stockage central des identités de leurs employés. À partir de là, le service informatique dispose souvent de processus efficaces pour le provisioning et le déprovisioning des employés, ce qui permet de contrôler automatiquement l'accès en fonction des besoins et des rôles. Sur site ou dans le cloud, le contrôle des informations confidentielles se justifie par les mêmes facteurs commerciaux déterminants. En l'absence de contrôle, votre entreprise est vulnérable.

En matière de cloud, vos utilisateurs bénéficient-ils d'une expérience simplifiée ? Il y a plusieurs années, les services informatiques ont compris que simplicité et facilité d'utilisation étaient la clé de la sécurité. Lorsque l'accès aux informations et applications sécurisées et la mémorisation de mots de passe sont trop complexes, les utilisateurs se créent leurs propres pense-bêtes sur des bouts de papier. Le Single Sign-on est venu remédier à ce problème. Les utilisateurs accèdent à leurs applications et informations rapidement et en toute simplicité. Simultanément, la sécurité de leurs applications est optimisée. Comment vous situez-vous en matière de Single Sign-on pour vos applications en nuage ? Les bouts de papier sont-ils de retour dans vos bureaux ?

Contrôle des risques dans le cloud

Les faibles obstacles à l'utilisation des applications SaaS et l'agilité commerciale qu'elles offrent sont la garantie de leur longévité. La question qui se pose est donc la suivante : comment les services informatiques doivent-ils s'adapter ? Les services informatiques doivent sécuriser les secrets de l'entreprise, les informations relatives aux clients ainsi que toutes les données réglementées que l'entreprise détient. Les principales fonctions applicables à la plupart des environnements sont énumérées ci-après.

Même si vous ne contrôlez pas les ressources, vous pouvez en contrôler l'accès. Pour garantir la sécurisation des données des clients et de l'entreprise, vous devez étendre la gestion des accès au-delà des limites de l'entreprise. De la même façon que le service informatique a fait évoluer ses processus pour vos applications internes, il doit contrôler l'accès des utilisateurs dans le cloud. Par ailleurs, puisque vos employés utilisent de plus en plus leurs périphériques mobiles personnels dans un cadre professionnel, la gestion des accès par le service informatique doit aussi inclure ces périphériques.

La clé de la sécurité des références d'entreprise est de les maintenir sous votre contrôle et votre protection, et jamais dans le cloud. Les solutions qui répliquent les références utilisateur hors site sont synonymes d'augmentation des risques pour vos informations et par conséquent votre entreprise. Inversement, les solutions les plus sécurisées ne permettent jamais aux utilisateurs de placer des références d'entreprise dans le cloud.

Étendez au cloud vos processus automatisés. Les processus adaptés à la gestion de votre environnement sont le fruit de nombreuses années de développement du service informatique. Il est par exemple courant aujourd'hui pour les entreprises de mettre en place un ensemble de processus et de stratégies pour leurs annuaires, qui sont souvent des implémentations Active Directory. Au sein de l'entreprise, le service informatique peut alors disposer de connexions avec d'autres zones de stockage d'identités qui contrôlent l'accès aux ressources et aux applications en fonction du rôle de chacun. Ces connexions constituent des points de synchronisation qui automatisent le contrôle des accès.

Les processus informatiques de contrôle des accès aux applications hébergées dans le cloud doivent être automatisés de la même manière que les processus d'accès internes. En matière de contrôle des accès autorisés aux applications SaaS, l'approche la plus sécurisée consiste à étendre les processus informatiques existants pour inclure les applications hébergées dans le cloud. Cette approche préserve également les investissements informatiques actuels.

Faites la chasse aux mauvaises habitudes. Pour éviter la réapparition rapide de pratiques d'authentification peu orthodoxes dans votre entreprise, vous devez étendre vos fonctions Single Sign-on à vos applications SaaS. Dans le cas contraire, les utilisateurs recommenceront à écrire leurs mots de passe sur des bouts de papier ou à les enregistrer dans des fichiers texte non sécurisés. La centralisation des mots de passe dans votre coffre-fort d'identité sécurisé est aussi cruciale que la conservation de vos références hors du cloud. Le Single Sign-on est la solution. Il garantit la simplicité du processus d'authentification des utilisateurs, qui n'ont pas besoin de mémoriser des mots de passe supplémentaires. La sécurité est préservée et l'expérience utilisateur est également améliorée.

Plutôt que de transférer les références des utilisateurs vers le cloud, les solutions de Single Sign-on correctement déployées conservent ces références sur site et sous votre contrôle. Malgré la simplicité de l'expérience utilisateur, en arrière-plan, des références uniques générées par un ordinateur sont utilisées par la passerelle d'authentification auprès des applications en nuage. Non seulement les références secrètes restent confidentielles, mais la solution contrôle le comportement des utilisateurs, qui doivent accéder au cloud via la passerelle.

Audit et création de rapports. Selon le type d'applications et d'informations que votre entreprise conserve dans le cloud, un même niveau d'audit et de création de rapports peut être requis pour vos environnements SaaS et pour vos applications internes. Dans le cadre du suivi des principales métriques, il est important de savoir qui dispose de privilèges d'accès, qui a accédé aux applications et à quel moment. Pour les informations réglementées, la démonstration de conformité est aussi essentielle que la conformité elle-même.

Aspects incontournables de l'adoption

L'implémentation doit être rapide. Vos employés utilisent un large éventail de technologies, c'est pourquoi le service informatique est souvent réticent à l'adoption de solutions difficiles à déployer. Quelques jours ou semaines peuvent vous suffire pour déployer des applications bien conçues qui utilisent les technologies de virtualisation actuelles, car vous pouvez contourner le processus d'installation. De plus, la configuration est simplifiée. Ainsi, la solution adéquate doit être opérationnelle en quelques jours, contrairement aux projets de datacenters traditionnels qui peuvent nécessiter plusieurs mois.

La maintenance doit être allégée. Dans un contexte où les budgets informatiques sont au mieux gelés mais le plus souvent en diminution, des solutions de gestion complexes ou coûteuses à mettre à jour et à maintenir sont inadaptées. Une fois approuvées, les meilleures solutions fournissent des workflows de mise à jour aux administrateurs et des mises à jour automatiques avec retour à l'état initial.

Sélection d'une solution

La sélection du fournisseur approprié est tout aussi importante que le choix des outils de gestion des accès aux applications SaaS. Voici quelques points à prendre en compte lors de la sélection d'un fournisseur.

- **Crédibilité**. Quelle est la réputation du fournisseur sur le marché ? Dans quelle mesure ses autres clients sont-ils satisfaits de son support et de ses services ? Si sa réputation est douteuse ou s'il est trop nouveau dans le secteur pour s'en être forgé une, soyez encore plus vigilant lors du processus de sélection.
- **Vision pour l'avenir**. Quelles sont les perspectives du fournisseur ? Se comporte-t-il plutôt comme un leader ou un suiveur ? Sa vision coïncide-t-elle avec la vôtre ?
- **Leadership et historique**. Quel est l'historique du fournisseur ? A-t-il innové sur son marché ? A-t-il démontré qu'il s'intéressait de près au marché du cloud et des solutions SaaS ou semble-t-il y avoir pensé après coup ?
- **Performances établies**. Là encore, comment les clients existants du fournisseur évaluent-ils ses performances ? Le personnel de support et les ingénieurs du fournisseur s'y connaissent-ils dans leur domaine respectif ? Ce fournisseur a-t-il déjà implémenté avec succès des solutions semblables aux vôtres sur d'autres sites ?

En raison de l'accélération du rythme d'adoption des applications SaaS, il est plus que jamais essentiel de choisir soigneusement vos produits, tout comme l'entreprise qui les prend en charge. Des processus adéquats de recherche, de planification et de sélection de partenaires garantissent la réussite de votre entreprise pour les années à venir.

Votre réussite est notre priorité

NetIQ travaille en étroite collaboration avec chaque entreprise afin d'identifier clairement et immédiatement ses besoins et points faibles. Notre expérience en termes de distribution de solutions informatiques capables de répondre aux changements continus, à la complexité et aux risques (au sein d'entreprises telles que la vôtre) est au final ce qui vous permet de surmonter ces obstacles et de proposer des services métiers efficaces.

L'engagement de NetIQ à fournir un service clientèle exceptionnel et des solutions innovantes, ainsi qu'une équipe conviviale, sont au coeur de chaque déploiement. Pour toutes ces raisons, NetIQ est en mesure de satisfaire les besoins tactiques et stratégiques de ses clients et partenaires.

NetIQ peut contribuer à votre réussite

Les solutions innovantes, les produits de qualité et le service exceptionnel de NetIQ assurent la prise en charge des besoins tactiques et stratégiques de ses clients. Nos objectifs sont la réussite de nos clients et leur fidélisation à long terme. Notre culture d'entreprise et nos processus fournissent aux clients une expérience positive qui simplifie les interactions commerciales avec NetIQ.

Plus grande que les fournisseurs de solutions ponctuelles, la société NetIQ dispose de ressources dont ils sont dépourvus, mais elle conserve néanmoins une taille humaine. Nous répondons aux besoins des clients rapidement et directement.

À propos de NetIQ

NetIQ est un fournisseur international de logiciels informatiques d'entreprise dont les efforts sont constamment axés sur la réussite de ses clients. NetIQ comble, à moindres frais, les besoins de ses clients et partenaires en matière de protection des informations. De plus, notre société gère les aspects complexes des environnements d'applications dynamiques hautement distribués.

Notre portefeuille comprend des solutions automatisées et évolutives, spécialisées dans la gestion des identités, de la sécurité et de la gouvernance, ainsi que des opérations informatiques. Les entreprises sont ainsi en mesure de fournir, mesurer et gérer en toute sécurité des services informatiques à l'échelle de leurs environnements physiques, virtuels et en nuage (cloud computing). Associées à notre approche pratique et orientée client de la résolution des problèmes informatiques récurrents, ces solutions aident les entreprises à réduire les coûts, la complexité et les risques.

Pour en savoir plus sur nos solutions logicielles reconnues par les professionnels du secteur, visitez le site **www.netiq.com**.

France
Tour Franklin
100/101, Quartier Boieldieu
92042 Paris la Défense Cedex
France
Tel: +01 55 62 50 00
Fax: +01 55 62 51 99

Email : contact-fr@netiq.com
info@netiq.com
www.netiq.com
http://community.netiq.com

Pour obtenir la liste complète de nos bureaux d'Amérique du Nord, d'Europe, du Moyen-Orient, d'Afrique, d'Asie-Pacifique et d'Amérique latine, visitez la page : **www.netiq.com/contacts**.