APIXIT

L'expertise augmentée

4 ÉTAPES VERS LA GESTION DES ACCÈS CLOUD

Un guide détaillé et pratique sur la gestion des accès Cloud dans votre entreprise

Janvier 2023

THALES

DÉFIS LIÉS À L'ACCÈS AU CLOUD

Les applications cloud sont maintenant courantes dans les entreprises : 93 % des organisations utilisent des services IT basés dans le cloud[1].

Exploiter des applications cloud comporte cependant certains défis. Les applications cloud étant ce qui se fait de mieux et permettant un retour sur investissement rapide, les entreprises les adoptent très vite, mais elles sont perplexes devant la complexité croissante de leur utilisation et de leur gestion.

Lassitude liée aux mots de passe

Les utilisateurs ont de nombreux noms d'utilisateur et mots de passe à gérer. Ils doivent s'authentifier plusieurs fois par jour et finissent souvent par contourner les stratégies de sécurité.
Il en résulte une lassitude engendrée par le besoin incessant de créer, mettre à jour et réinitialiser des mots de passe pour différentes applications, et ce, tous les jours.

Sécurité médiocre

Les applications cloud ne sont protégées que par des mots de passe faibles et statiques, fait qui peut compromettre la confidentialité des informations confidentielles et augmenter les risques de brèche. La majorité des vols de données peut être contrecarrée à l'aide d'une robuste authentification à deux facteurs[2].

Gestion complexe

À chaque nouvelle application cloud, c'est une nouvelle console ou un autre portail d'administration à comprendre pour gérer et dépanner les utilisateurs.
Si une entreprise utilise une dizaine d'application ou plus, les efforts requis pour l'administration deviennent colossaux.

Risque de non-conformité

Démontrer sa conformité aux réglementations requiert une entière visibilité des activités d'accès. Un service informatique doit savoir qui accède à quelle application et quand.
De plus, comme les applications cloud contiennent des données confidentielles, les administrateurs doivent savoir comment l'identité des utilisateurs est vérifiée.

Coûts d'assistance élevés

Le nombre croissant d'identités cloud et d'informations d'identification engendre des réinitialisations fréquentes des mots de passe. Ces dernières représentent 20 % des coûts d'assistance d'une entreprise[3].

1 Étude de Spiceworks : 93 Percent of Organizations Use Cloud-Based IT Services (93 % des entreprises utilisent des services informatiques dans le cloud)

2 Rapport d'enquête 2016 sur les brèches de données de Verizon

3 Statisnet, Forgotten user passwords – Eliminate the Problem Dramatically Reduce the Cost (Mots de passe oubliés : éliminer le problème réduit considérablement les coûts)

QUATRE ÉTAPES VERS LA GESTION DES ACCÈS CLOUD

ÉTAPE 1 – MISE EN PLACE D'UNE AUTHENTIFICATION CLOUD UNIQUE (SSO)

Pour faciliter la vie des utilisateurs et pour libérer le service informatique des réinitialisations des mots de passe, mettez en place le single sign on cloud pour toutes les applications cloud de votre entreprise.

Qu'est-ce que l'authentification unique ou single sign on ?
L'authentification unique (aussi appelée Single Sign On ou SSO) permet de s'authentifier une première fois et d'être ensuite authentifié automatiquement lorsque vous accédez à différentes ressources.
Vous n'avez alors plus besoin de vous connecter et de vous authentifier pour chaque système et chaque application. C'est un d'intermédiaire entre l'utilisateur et les applications cibles.

Avec le single sign on (SSO), les utilisateurs se connectent une seule fois pour avoir accès simultanément à toutes les applications cloud. Ils se connectent avec leur identité d'entreprise, celle qu'ils utilisent lorsqu'ils se connectent au réseau le matin ou au VPN le soir.

Adapter le SSO aux rôles
Les utilisateurs et les groupes d'utilisateurs requièrent l'accès à différentes applications cloud. L'authentification unique peut être appliquée sur les applications cloud selon les besoins de chaque équipe, de chaque rôle, de chaque service et de chaque utilisateur.
Par exemple, en plus des applications de l'entreprise, le service R&D peut avoir besoin d'accéder à des applications comme Jira, Confluence et AWS alors que le marketing a besoin d'accéder à Salesforce, Office 365 et WordPress. Les partenaires commerciaux, comme les sous-traitants et les fournisseurs, ont peut-être besoin d'accéder à un nombre réduit d'applications cloud telles que les portails partenaires et les suites de bureautique.

Créez des groupes d'utilisateurs basés sur le rôle dans votre magasin d'utilisateurs d'entreprise, que ce soit Active Directory, My SQL ou autre référentiel, pour simplifier la configuration des stratégies d'accès basées sur les groupes.

Les groupes basés sur les rôles facilitent également la mise en service, la mise à jour et la révocation des autorisations d'accès lorsque des utilisateurs rejoignent ou quittent l'entreprise, ou changent de poste.

Avantages du SSO : Confort, gestion facile et conformité
Le SSO fournit non seulement un accès pratique et transparent aux utilisateurs, mais facilite également la vie de l'administrateur en lui permettant de maintenir une seule identité (un seul nom d'utilisateur et un seul mot de passe) par utilisateur, pour toutes les ressources cloud. Ainsi, plus de besoin de réinitialiser les mots de passe et il n'y a plus de coûts de dépannage des utilisateurs à cause des différentes consoles d'administration.

Grâce à la vue unique sur les événements d'accès, le service IT peut observer qui accède à quelle ressource, quand et avec quelle méthode d'authentification.
Il est ainsi plus facile de s'assurer de la conformité réglementaire et de la sécurité. Grâce à la vue unifiée de l'accès au cloud, vous pouvez également identifier les licences sous-utilisées.

Le concept d'authentification unique a été mis en place depuis longtemps pour les applications, portails et réseaux sur site (par exemple à l'aide du protocole Kerberos). Grâce à l'évolution des protocoles de fédération des identités (comme le protocole SAML 2.0) qui étend les identités d'entreprise au cloud, les entreprises bénéficient des avantages de ce type de protocole pour leurs ressources cloud.

Avec l'authentification unique (SSO), les utilisateurs se connectent une seule fois pour avoir accès simultanément à toutes les applications cloud.

Étape 2 – protection des identités grâce aux stratégies d'accès granulaires

Le SSO facilite la vie des utilisateurs et la gestion pour l'IT, mais il ne résout qu'une partie des problèmes liés à la gestion de l'accès au cloud. L'authentification unique permet d'avoir une seule identité pour chaque utilisateur pour toutes les applications cloud et de gérer cette identité, mais que se passe-t-il si une identité est compromise ? C'est dans cette situation que les stratégies d'accès basées sur le scénario prennent toute leur importance. Avec elles, vous pouvez déterminer le niveau adéquat d'authentification, pour le bon utilisateur, au bon moment.

Stratégies d'accès basées sur des scénarios
Nous connaissons tous l'authentification à deux facteurs (2FA). Cette dernière peut cependant être excessive dans le cas des applications à faible risque auxquelles les utilisateurs accèdent depuis le réseau d'entreprise et d'autres scénarios d'accès similaires. Pour protéger les identités uniques au niveau de confiance adéquat vous pouvez donc mettre en oeuvre des stratégies d'accès granulaires de manière à ce qu'elles s'alignent sur le niveau d'authentification du scénario concerné. Par exemple, le niveau de confiance requis pour une application de gestion du temps à faible risque peut différer du niveau requis lors d'une connexion à une ressource sensible comme le VPN de l'entreprise. De même, se connecter au compte d'un administrateur informatique ou au compte du PDG peut demander une sécurité renforcée.

Comme les applications ne requièrent pas toutes le même niveau de sécurité et comme les utilisateurs n'ont pas tous besoin des mêmes privilèges de compte, vous pouvez définir des stratégies d'accès basées sur le scénario. Ces dernières prennent en compte le niveau de confidentialité et d'exposition aux risques d'une application cloud ainsi que les privilèges des différents groupes d'utilisateurs. Par exemple les administrateurs IT et les cadres dirigeants.

Lorsque le niveau de confiance est bas, par exemple lors d'une connexion à partir d'un réseau inconnu, la sécurité peut être renforcée avec un facteur d'authentification supplémentaire comme une méthode d'authentification hors bande ou autre méthode à deux facteurs.Lorsque le niveau de confiance est élevé, par exemple lors d'une connexion à partir du réseau de l'entreprise et avec un appareil connu, l'utilisateur obtient un accès

Exploitation des informations contextuelles pour l'authentification continue
En tirant parti des informations contextuelles (p. ex. l'utilisateur se connecte à partir d'un réseau de confiance ou un appareil connu), les solutions de gestion des accès garantissent une expérience utilisateur vraiment pratique, c'est-à-dire que l'authentification est renforcée uniquement dans les situations à haut risque. Les utilisateurs passant de leur ordinateur à leur tablette tout au long de la journée, la stratégie d'accès doit être adaptée et appliquée à l'application à laquelle ils se connectent, à l'équipe dont ils font partie et aux informations contextuelles
glanées sur leur comportement... C'est ainsi que l'authentification continue est assurée au niveau de confiance adéquat tout au long de la journée.

Le niveau de confiance requis pour une application de gestion du temps à faible risque peut différer du niveau requis lors d'une connexion à une ressource sensible comme le VPN de l'entreprise.

Après avoir appliqué l'authentification unique à toutes les applications cloud utilisées par chacun des groupes d'utilisateurs (cadres dirigeants, R&D, vente, exploitation, etc.), il vous faut mettre en oeuvre des stratégies d'accès basées sur le scénario qui adaptent la méthode d'authentification au scénario rencontré. Ainsi, chaque connexion est vérifiée et l'accès reste transparent.

D'une stratégie globale à une stratégie granulaire
Pour simplifier la configuration des stratégies d'accès, envisagez de commencer avec une seule stratégie globale, puis ajoutez-y des exceptions selon les besoins.

Votre stratégie globale sert de stratégie d'accès par défaut pour toutes les applications cloud et pour tous les utilisateurs. Elle demande aux employés de se connecter une fois à chaque session d'authentification unique à l'aide d'un mot de passe à usage unique et ensuite l'utilisateur n'a plus à s'authentifier lorsqu'il se connecte à ses applications web et cloud.

Une fois la stratégie globale en place, vous pouvez définir des exceptions demandant une authentification renforcée pour les scénarios à haut risque, par exemple lors de l'accès à une application sensible en dehors du réseau.
Les applications non sensibles, quant à elles, utilisent uniquement les contrôles d'accès par défaut définis dans la stratégie globale.

Étape 3 – optimisation des stratégies d'accès grâce aux informations découlant des données

Comment savoir si vos stratégies d'accès sont trop tolérantes, trop pesantes ou vraiment adaptées ? C'est grâce aux informations déduites des données que vous le saurez. En examinant les applications auxquelles les utilisateurs accèdent tout au long de la journée, qui y accède et avec quelle stratégie d'accès, le service IT peut ajuster les stratégies d'accès basées sur le scénario.

Si les utilisateurs accèdent souvent à une application sensible à partir d'un réseau inconnu ou d'un emplacement à haut risque (comme l'indique la fréquence à laquelle la stratégie est mise en oeuvre), le service informatique peut modifier la stratégie de façon à augmenter le niveau de confiance requis pour accéder à telle ou telle application.
Si la stratégie ne demandait qu'un mot de passe ou code PIN jusqu'à maintenant, elle peut être ajustée pour demander la saisie d'un code secret à usage unique.

Inversement, si tous les utilisateurs passent fréquemment par une stratégie d'accès demandant un mot de passe et un mot de passe à usage unique, il est peut-être envisagé de simplifier la connexion en demandant des informations d'identification simples (nom d'utilisateur et mot de passe à usage unique) et d'utiliser les informations contextuelles pour définir s'il y a besoin d'informations d'authentification supplémentaires.

L'intégration des données statistiques aux stratégies d'accès aide les entreprises à mettre en place une gestion des risques efficace et à trouver le juste milieu entre sécurité et facilité d'utilisation.

Étape 4 – évolutivité de votre infrastructure cloud

Combien d'applications cloud votre entreprise prévoit-elle d'ajouter l'année prochaine ? Une fusion ou un achat sont-ils en vue ? Lorsque vous évaluez les solutions de gestion d'accès au cloud, assurez-vous de pouvoir faire évoluer votre solution afin d'ajouter facilement des groupes d'utilisateurs et de nouvelles
applications cloud selon les besoins.

Les normes du secteur comme SAML 2.0 sont prises en charge par la plupart des services cloud. Elles vous permettent de faire évoluer la gestion des accès au cloud au fur et à mesure que vous adoptez de nouvelles applications. Les modèles d'intégration inclus simplif.

SafeNet Trusted Access – le moyen intelligent de gérer les accès au cloud

SafeNet Trusted Access est un service de gestion des accès, qui associe le confort du SSO à une sécurité granulaire des accès. En validant les identités, et en appliquant des stratégies d'accès ainsi qu'une identification unique et intelligente, les entreprises peuvent garantir un accès sécurisé et pratique à de nombreuses applications cloud à partir d'une console unique et conviviale.

Elles réduisent ainsi les coûts de gestion en définissant et en appliquant des contrôles d'accès de manière centralisée à partir d'une seule console conviviale.

Grâce à sa configuration rapide et facile, SafeNet Trusted Access simplifie le passage au cloud et améliore la visibilité et la conformité. Elle permet également une grande évolutivité via les flux de travail simplifiés fournis via le cloud.

Avec ses contrôles d'accès et d'authentification souples et personnalisables, SafeNet Trusted Access facilite la vie des utilisateurs, car ils n'ont qu'une seule identité d'entreprise à utiliser pour accéder à toutes leurs applications cloud.

À PROPOS DES SOLUTIONS SAFENET D'ACCESS MANAGEMENT ET D'AUTHENTIFICATION DE THALES

Les solutions de gestion des accès et d'authentification de Thales, leaders sur leur marché, permettent aux entreprises de gérer et protéger les accès aux applications IT, web et cloud de l'entreprise de façon sécurisée. En utilisant un SSO basé sur des stratégies et des méthodes d'authentification universelles, les entreprises peuvent prévenir de façon efficaces les brèches, migrer vers le cloud en toute sécurité et simplifier la mise en conformité.

Pour en savoir plus sur l'access management par Thales, consultez thalesesecurity.com/thales-gemalto

A PROPOS D'APIXIT

Depuis plus de 30 ans, APIXIT éclaire la Cybersécurité, les Infrastructures et le Cloud des ETI et des Grands Comptes.

En matière de protection du Système d'Information, notre proposition de valeur s'articule autour d'une démarche de Sécurité Opérationnelle alliant solutions technologiques d'éditeurs leaders du marché et offre de services à forte valeur ajoutée.

APIXIT vous accompagne sur l'ensemble du cycle de vie de vos solutions au travers de prestations d'audit et conseil, d'intégration, de MCO et MCS ou encore de Services Managés et de services SOC.

Grâce à leur sens de l'écoute et du service, nos équipes d'experts s'engagent à répondre avec agilité aux enjeux de transformation digitale de nos clients.

THALES

APIXIT
L'expertise augmentée

AMERICAS
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

ASIA PACIFIC – THALES TRANSPORT & SECURITY (HK) LTD
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

EUROPE, MIDDLE EAST, AFRICA
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.co

Les Conquérants, Immeuble Annapurna
1 Av. de l'Atlantique
91940 Les Ulis
Tel : 01 64 86 97 97