thalesgroup.com

THALES

Adapter les stratégies de gestion des risques aux besoins des utilisateurs grâce à la gestion des accès Cloud

Alors que les solutions d'identification unique Single Sign-On (SSO) traditionnelles appliquent une stratégie globale à toutes les ressources cibles, les solutions de gestion des accès sont apparues pour offrir à la fois l'aspect pratique du SSO et la sécurité granulaire offerte par des stratégies d'accès personnalisables.

En appliquant le SSO aux applications Cloud et Web cibles, tout en affinant les contrôles d'accès et les besoins d'authentification selon des scénarios de cas d'utilisation spécifiques, les organisations peuvent offrir à leurs utilisateurs un accès fluide, tout en restant protégées et en conformité, et en gardant le contrôle.

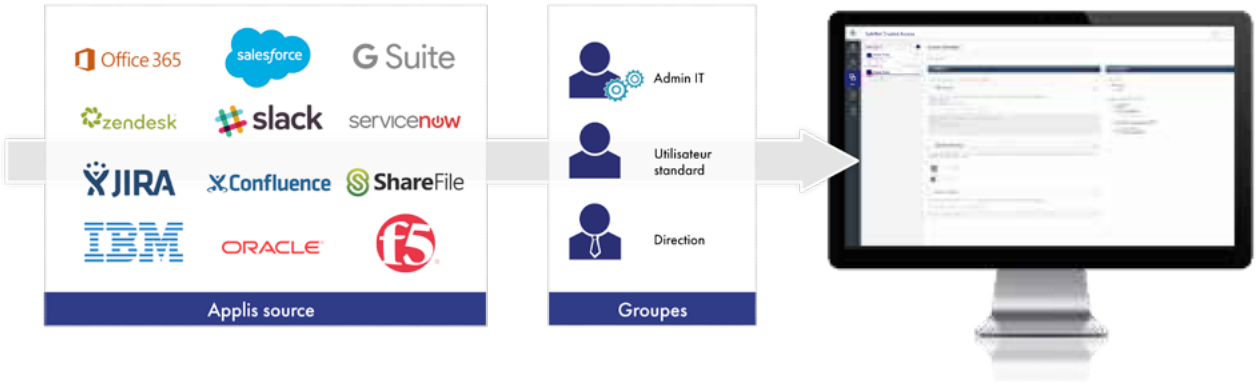
Sécurité granulaire des accès SSO

Lors de la configuration des stratégies pour les applications critiques, les organisations choisissent normalement des contrôles d'accès plus rigoureux afin de garantir qu'un utilisateur est bien la personne qu'il prétend être. Il en va de même pour la sécurisation des accès accordés aux utilisateurs à privilège, aux travailleurs distants, aux consultants ou aux prestataires externes ne faisant pas partie de l'entreprise. Et cela est également valable pour la sécurisation des accès depuis des pays où votre organisation ne mène normalement pas ses activités.

Ces scénarios de cas d'utilisation peuvent être facilement pris en compte grâce à des stratégies d'accès précises, dédiées et configurées pour les services Cloud et Web.

Appliquer des contrôles d'accès renforcés aux travailleurs nomades

Les travailleurs nomades qui se connectent en dehors du réseau de l'entreprise peuvent avoir besoin de facteurs d'authentification supplémentaires par rapport aux travailleurs sur site qui se connectent depuis leur bureau. Pour ce faire, une stratégie globale peut être définie. Seul un mot de passe de domaine est alors requis pour les utilisateurs qui lancent une session SSO depuis le bureau, dans le réseau d'entreprise. Une stratégie d'exceptions peut être ajoutée pour exiger un facteur d'authentification supplémentaire, comme un code secret à usage unique (OTP), pour tous les utilisateurs ne faisant pas partie du réseau connu et qui se connectent hors du bureau.



Ainsi, les utilisateurs qui se connectent au bureau le font uniquement à la session SSO avec un mot de passe de domaine et peuvent ensuite facilement passer d'une application à l'autre (à moins que la configuration ne le permette pas). À l'inverse, il sera demandé aux utilisateurs qui se connectent hors du bureau d'entrer un second facteur sous la forme d'un identifiant à usage unique OTP.

Appliquer des contrôles d'accès plus rigoureux aux applications critiques

Certaines organisations peuvent souhaiter proposer une identification unique pour la plupart de leurs applications, tout en exigeant des contrôles d'accès plus rigoureux pour les applications critiques qui hébergent des données sensibles ou qui se trouvent à la base d'infrastructures fondamentales. Pour apporter une solution à ce scénario, les administrateurs informatiques peuvent élaborer une stratégie exigeant une authentification uniquement à l'aide d'un mot de passe pour les utilisateurs qui accèdent à leur première application en début de journée. Une stratégie d'exceptions peut être ajoutée afin d'exiger une authentification supplémentaire pour les utilisateurs qui accèdent aux applications critiques. Par exemple, il est possible de demander aux utilisateurs d'entrer un OTP, ou bien d'approuver une demande de connexion envoyée sur leur appareil mobile.

Appliquer des contrôles d'accès plus rigoureux dans certaines zones géographiques

Les organisations préoccupées par l'accès à leurs applications depuis des sites où elles ne mènent habituellement pas leurs activités peuvent refuser les tentatives d'accès provenant de certains pays ou bien définir des contrôles d'accès plus rigoureux pour ces tentatives d'accès. Configurer des contrôles spécifiques pour les tentatives d'accès provenant de ces pays permet aux organisations de surveiller l'activité en provenance de certains endroits.

Par exemple, une stratégie d'exceptions peut être définie pour exiger une authentification multifactorielle chaque fois qu'une session SSO est lancée depuis l'un de ces sites identifiés.

Appliquer des contrôles d'accès renforcés aux consultants externes

Les entreprises qui souhaitent fournir à leurs utilisateurs principaux en interne une expérience SSO, tout en renforçant les contrôles d'accès pour les prestataires et les consultants extérieurs, peuvent le faire en configurant une stratégie basée sur ce groupe d'utilisateurs. Cette stratégie exigera un second facteur d'authentification chaque fois qu'une session de single sign-on sera lancée. De cette manière, les prestataires peuvent profiter d'un accès fluide à toutes leurs applications, tandis que le service informatique peut renforcer le niveau de fiabilité des sessions SSO lancées par ce groupe d'utilisateurs.

Une valeur stratégique pour votre entreprise

SafeNet Trusted Access est un service de gestion des accès au Cloud permettant une identification unique et sécurisée par l'application de stratégies d'accès précises.

En permettant aux administrateurs IT de créer des stratégies basées sur les cas d'utilisation, SafeNet Trusted Access leur apporte la flexibilité nécessaire pour protéger leur organisation et leurs applications sensibles sans impact négatif sur l'expérience SSO des utilisateurs finaux.

Les stratégies d'exceptions précises donnent la possibilité aux services informatiques des entreprises de renforcer la sécurité sur des applications, des sites géographiques ou des groupes d'utilisateurs spécifiques, tout en proposant une expérience d'accès fluide pour les utilisateurs et cas d'utilisation principaux.

En adaptant les stratégies d'accès au scénario auquel ils sont confrontés, les services IT peuvent garantir que les stratégies sont aussi rigoureuses ou flexibles qu'ils le souhaitent ; par exemple, en demandant une information d'identification, plusieurs ou bien aucune, chaque fois qu'un utilisateur se connecte à une session SSO ou à une application en particulier.

Pour en savoir plus sur la gestion des accès de Thales, rendez-vous sur la page https://safenet.gemalto.com/accessmanagement ou participez à un webinaire de démonstration en direct.

À propos de Thales

Les personnes à qui vous accordez confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.

Une technologie décisive pour des moments décisifs.

> thalesgroup.com <

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) Lt, 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 – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com