

Contrôle et sécurité des applications SaaS

Les applications SaaS – de Dropbox Business à Salesforce.com, en passant par Office 365 – deviennent de plus en plus populaires, mais elles impliquent de nouveaux risques quant à la sécurité et à la conformité. Le «Cloud Access Security Broker» Aperture de Palo Alto Networks y remédie.

Il est très pratique d'utiliser des services SaaS basés sur le cloud, au lieu d'installer et d'entretenir à grands frais des logiciels sur des serveurs propres à l'entreprise. C'est ce qui explique leur popularité. Du stockage de données avec les éditions Business de Dropbox, Google Drive, etc. aux applications d'entreprise comme Salesforce.com, en passant par la gestion de code source avec Github: les applications SaaS sont devenues indispensables.

Bien que ces services soient très utiles, ils présentent aussi des risques majeurs: les applications SaaS sont souvent mises en service directement et de manière incontrôlée par les services, en passant outre le service IT. Les données sensibles ne sont ainsi plus stockées au sein de l'entreprise, mais largement distribuées chez différents fournisseurs de cloud. Souvent, les utilisateurs individuels eux-mêmes ne savent plus très bien quelles données sont stockées à quel endroit. Pour



Aperture de Palo Alto Networks offre une protection complète aux applications SaaS et documents figurant dans le cloud.

l'architecture de sécurité IT existante, les services SaaS et les données traitées par leur biais sont par ailleurs invisibles. De plus, les règles en vigueur au sein du service IT de l'entreprise sont contournées lors de l'utilisation de SaaS. Et il y a un risque que des logiciels malveillants soient introduits dans le réseau de l'entreprise suite à un échange de données irrégulier.

Aperture renforce le contrôle des applications SaaS

Pour que les applications SaaS soient intégrées dans le paysage informatique de manière sécurisée et conforme, un outil approprié est indispensable. Les responsables d'études de marché de Gartner nomment de tels outils «Cloud Access Security Broker» – ces derniers fonctionnent donc comme des agents garantissant un accès sécurisé aux services basés sur le cloud. Aperture de Palo Alto Networks répond de manière optimale aux exigences impliquées.

Cette solution garantit une visibilité complète de toutes les activités liées aux utilisateurs de services SaaS et des fichiers et répertoires concernés – et cela tout au long du cycle de vie d'un compte d'utilisateur SaaS. Il en résulte un Audit Trail complet pour chaque utilisateur: on voit clairement, jusqu'au moindre détail, qui a partagé quoi et quand et pendant combien de temps avec qui. Et on peut réaliser des analyses rétrospectives – que les activités examinées aient eu lieu il y a une heure ou des années auparavant.

En outre, Aperture ne surveille pas uniquement les accès, mais scanne et analyse également les contenus qui sont traités par le biais des services SaaS. De plus, Aperture classe automatiquement les documents. Cela permet d'identifier si un document comporte des informations juridiquement pertinentes ou des secrets d'affaires et doit donc être traité en conséquence. Bien que l'administrateur Aperture puisse

rechercher activement toutes failles de sécurité et définir des alertes automatiques, il n'a aucun accès aux documents réels. Important: le processus de numérisation peut être adapté aux lois européennes relatives à la protection des données.

Lors de l'évaluation d'un problème potentiel de sécurité, Aperture fournit une vision claire. Finies donc les spéculations! L'entreprise sait exactement et à tout moment ce qui est arrivé à ses données et détecte rapidement toute violation des règles de conformité et de protection des données. Aperture offre également une protection intégrée contre les logiciels malveillants, basée sur le cloud Wildfire de Palo Alto Networks.

Un service cloud utilisable de manière universelle

En tant que pur service cloud, Aperture ne nécessite aucune modification du réseau d'entreprise ni installation de logiciel et est complètement transparent pour les utilisateurs. Le service communique directement avec les solutions SaaS en utilisant les API natives des applications individuelles.

Aperture complète la vaste plate-forme de sécurité de Palo Alto Networks en y ajoutant la nouvelle dimension du Cloud Access Security Broker, mais le service peut également être utilisé indépendamment, dans des environnements qui n'utilisent aucun autre produit Palo Alto Networks.

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
contact@boll.ch / www.boll.ch

APERTURE: LES POINTS FORTS

- Utilisation sécurisée et contrôlée des applications SaaS
- Visibilité complète de toutes les activités liées aux utilisateurs SaaS, fichiers et répertoires
- Analyse rétroactive de l'ensemble du cycle de vie des comptes d'utilisateurs SaaS
- Livraison d'un aperçu en temps opportun des violations de la protection des données et de la conformité
- Surveillance et application granulaires et adaptées au contexte des règles d'entreprise
- Protection intégrée contre les logiciels malveillants connus et inconnus