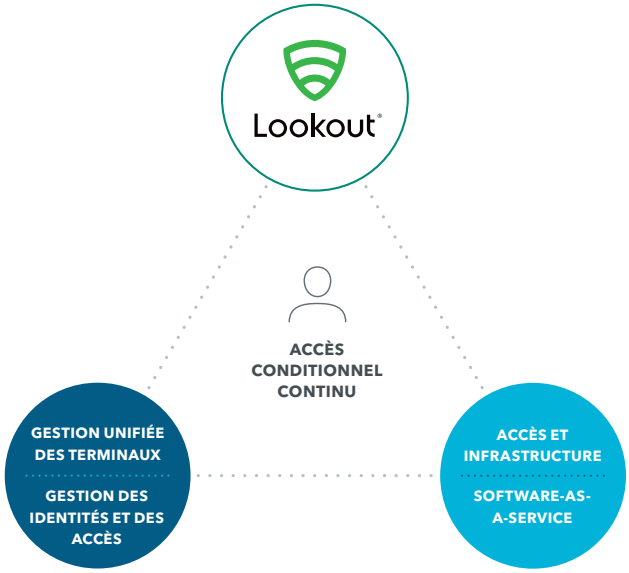
Lookout assure un accès conditionnel continu

À l'heure où les employés accèdent à des données sensibles d'entreprise via des applications et des appareils mobiles, les organisations doivent trouver un moyen de veiller en continu à ce que les appareils restent sains.

Des défis de sécurité à l'échelle du secteur

Comme les organisations dépendent de plus en plus de la mobilité pour dynamiser la productivité de leurs employés, il est nécessaire de les protéger contre les risques associés à l'accès à des données d'entreprise à partir des terminaux mobiles. Certaines plateformes de gestion mobile mettent à jour les détails des applications toutes les quatre heures seulement, et les solutions de gestion des identités et des accès renouvellent leurs jetons d'identité toutes les 24 heures seulement. Il est donc difficile de bénéficier d'une visibilité continue sur les appareils que les employés utilisent pour accéder aux infrastructures et aux données d'entreprise.



Visibilité continue : un besoin réel

Étant donné que des attaques telles que le phishing mobile et l'exploitation des vulnérabilités des appareils peuvent se dérouler en quelques secondes seulement, sans que l'utilisateur ne s'en rende compte, Lookout évalue en continu l'état de santé de tous les appareils qui accèdent aux données d'entreprise en surveillant de façon dynamique l'état de santé d'un terminal lorsqu'un utilisateur est connecté à l'entreprise. En utilisant l'accès conditionnel continu pour surveiller les risques et la confiance, les organisations ont la possibilité d'autoriser seulement les appareils sains à se connecter aux plateformes sur lesquelles sont stockées des données sensibles, ce qui élimine la menace que représentent les risques liés à l'appareil, à l'application ou au réseau.

La fonctionnalité stratégique de Lookout

Selon IDC, la fuite ou l'exposition de données sensibles représente l'un des principaux incidents de sécurité associés aux appareils mobiles auxquels les organisations ont été confrontées au cours de l'année passée[1]. En utilisant l'accès conditionnel continu de Lookout, qui surveille de façon dynamique l'état de santé d'un terminal dès lors qu'un utilisateur est connecté à des ressources d'entreprise, vous protégez en permanence vos données professionnelles de valeur contre la fuite ou l'exposition sur vos appareils mobiles.

Pourquoi choisir Lookout ?

Lookout Mobile Endpoint Security assure la sécurité et la conformité continues de tous les appareils grâce à un ensemble de données considérable, alimenté par plus de 170 millions d'appareils et l'analyse de plus de 70 millions d'applications mobiles. Lookout Security Cloud facilite le déploiement de Lookout et la mise en place de politiques de sécurité dans l'ensemble de l'organisation, tant pour les appareils gérés que pour les appareils non gérés. Les utilisateurs reçoivent en temps réel des alertes et des étapes à suivre pour corriger les problèmes concernant les applications malveillantes, les connexions au réseau et les anomalies du système. Ils bénéficient également d'une vérification continue de l'état de santé de l'appareil afin d'assurer un accès conditionnel continu aux applications et aux données sensibles d'entreprise, ce qui permet de veiller à ce que les appareils des employés ne soient pas exploités par des acteurs malveillants dans le but de voler des ressources.

[1] IDC Enterprise Mobility Decision Maker Survey 2018, Nov. 2018 : https://www.idc.com/getdoc.jsp?containerId=US44434018

lookout.com/fr