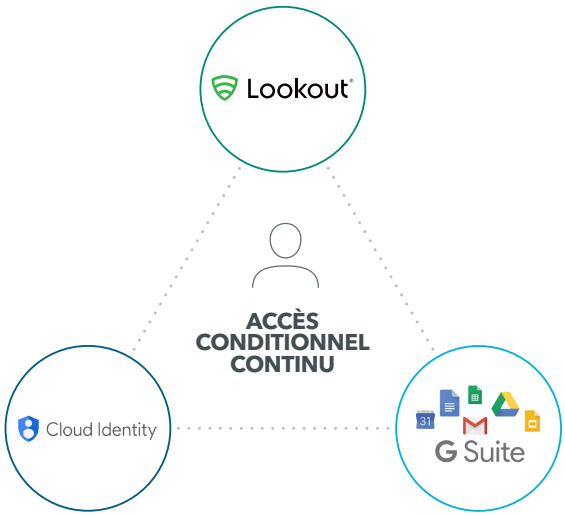
Lookout + Google Cloud

Sécurisez votre environnement extra-périmétrique avec Lookout et Cloud Identity

Au vu de la place prépondérante qu'occupe la mobilité au sein des organisations pour dynamiser la productivité des employés, la sécurité extra-périmétrique devient une priorité. Il s'agit d'une nouvelle stratégie de sécurité d'entreprise centrée sur la protection des données d'entreprise auxquelles accèdent les utilisateurs et appareils situés en dehors du périmètre de sécurité « traditionnel » de l'entreprise. La sécurité extra-périmétrique contrôle l'accès à Internet et aux données d'entreprise en évaluant en permanence les risques, puis modifie l'accès pour protéger les données et les utilisateurs si les niveaux de risque sont trop élevés.



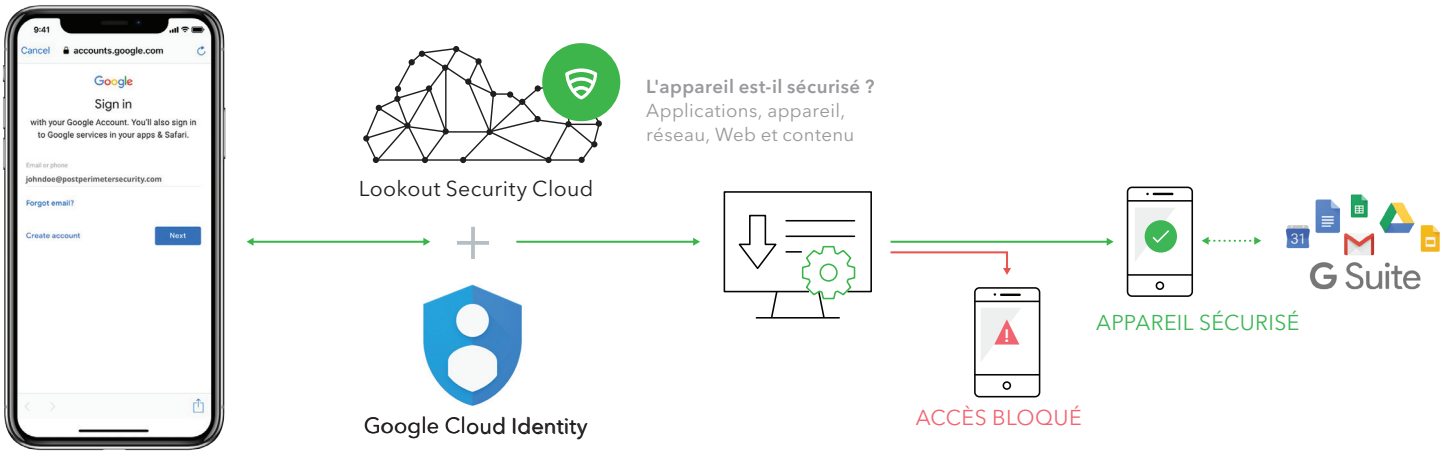
Ensemble, Lookout et Cloud Identity s'assurent que seuls les appareils mobiles de confiance peuvent accéder aux outils G Suite, tels que Docs et Slides, auxquels sont intégrés Cloud Identity et Mobile Endpoint Security. Des centaines de millions de personnes, d'entreprises et d'organismes publics font confiance à l'accès conditionnel continu de Lookout qui surveille de manière dynamique la santé d'un terminal pendant qu'un utilisateur est connecté à l'entreprise. Ainsi, seuls les appareils de confiance sont autorisés à se connecter aux plates-formes stockant des données sensibles, sans qu'un terminal, une application ou des risques présents sur le réseau ne puissent les compromettre.

Lookout et Cloud Identity fournissent un accès mobile sécurisé

L'utilisation d'une solution comme Cloud Identity est primordiale pour créer un environnement de sécurité extra-périmétrique renforcé. Pour cela, vous devrez activer la gestion des accès et des identités, l'authentification unique, la gestion unifiée des terminaux et d'autres fonctionnalités de sécurité indispensables. Lookout fournit ainsi une fonctionnalité de sécurité supplémentaire en s'appuyant sur Cloud Identity et l'accès conditionnel continu, afin de vous protéger de toutes tentatives d'hameçonnage, d'une application malveillante et autres risques inhérents à l'utilisation des portables en entreprise. Ensemble, Cloud Identity et Lookout protègent l'accès aux données d'entreprise stockées dans G Suite contre toute menace malveillante connue et inconnue.

Risques	Lookout + Cloud Identity
Authentification non sécurisée	Nécessite l'authentification multifacteur et vérifie que l'appareil est suffisamment en bonne santé pour accéder à la plate-forme d'authentification unique et aux applications de l'entreprise
Distribution des applications non sécurisées	Permet une distribution sécurisée des applications placées en liste blanche, ainsi qu'une détection et correction automatique des applications violant des politiques de sécurité
Violations de politiques d'application	Créez des politiques mettant des applications sur liste noire et isolez l'appareil du réseau de l'entreprise en cas de violation des politiques mises en œuvre
Applications vulnérables et malveillantes	Détectez les applications utilisant des méthodes de stockage/transfert de données non sécurisées et ayant des comportements à risque susceptibles de dévoiler des données
Vulnérabilités et défauts de configuration sous-jacents du système d'exploitation	Obtenez une visibilité totale dans les systèmes d'exploitation obsolètes, les configurations d'appareils à risque et les détections des jailbreaks/roots
Attaques basées sur le réseau	Protégez-vous contre toute attaque réseau malveillante ciblant des données d'entreprise chiffrées en cours de transfert
Menaces pesant sur le Web et les contenus	Surveillez et bloquez toute tentative de phishing mobile via le Web et les contenus

L'accès conditionnel continu en action



Employé accédant à une ressource de l'entreprise, telle que G Suite, depuis son appareil

Lookout et d'autres sources basées sur des politiques définies par un administrateur vont transmettre l'état de santé des appareils à Cloud Identity

Permet aux administrateurs de configurer des politiques d'accès dans Cloud Identity en fonction des politiques en vigueur et de l'état de l'appareil sur lequel Lookout est installé.

À propos de Post-Perimeter Security Alliance™

La Post-Perimeter Security Alliance rassemble des entreprises leaders, telles que Google et Lookout, dont l'objectif commun est de garantir la sécurité et d'améliorer la productivité dans un monde moderne, sans périmètre et axé sur le cloud et la confidentialité. Aujourd'hui, il est difficile d'assurer une sécurité extra-périmétrique complète via un fournisseur unique. Grâce à ses fonctionnalités de sécurité intégrées au niveau des terminaux, du Cloud et de l'identité, la Post-Perimeter Security Alliance protège l'accès aux données d'entreprise tout en favorisant la productivité. Ensemble, ces solutions évaluent en permanence les risques pesant sur les données d'entreprise, mais aussi contrôlent et corrigent la présence de tels risques.

À propos de BeyondCorp Alliance

La BeyondCorp Alliance est un groupe de partenaires gérant et protégeant les terminaux qu'utilise Google Cloud pour fournir des données de posture d'appareils à une solution d'accès contextuel Google Cloud. Un accès contextuel permet aux organisations de définir et de faire appliquer un accès granulaire aux applications et infrastructures en fonction de l'identité d'un utilisateur et du contexte de sa demande. Lookout est membre de la BeyondCorp Alliance qui permet aux organisations de surveiller de manière dynamique la santé des terminaux connectés à l'entreprise et d'alimenter le moteur d'accès contextuel de Google Cloud avec les données obtenues.

À propos de Lookout

Lookout est une société de cybersécurité fournissant des solutions pour les environnements extra-périmétriques axées sur le cloud et les terminaux mobiles. S'appuyant sur le plus grand ensemble de données de code mobile au monde, Lookout Security Cloud fournit une visibilité complète des risques mobiles. Des centaines de millions de personnes, d'entreprises et d'organismes et partenaires publics font confiance à Lookout, tels qu'AT&T, Verizon, Vodafone, Microsoft, Apple et autres. Lookout a son siège social à San Francisco et possède des bureaux à Amsterdam, Boston, Londres, Sydney, Tokyo, Toronto et Washington, D.C.

Pour en savoir plus, veuillez contacter votre partenaire.

Lookout

lookout.com/fr