Lookout®

SÉCURISER L'ACCÈS À VOS APPLICATIONS AVEC UNE APPROCHE « ZERO TRUST »

ACCÈS DYNAMIQUE AUX APPLICATIONS ET DONNÉES D'ENTREPRISE AVEC LOOKOUT ZERO TRUST NETWORK ACCESS

Les employés travaillant à distance souhaitent un accès fluide à ce dont ils ont besoin

Une infrastructure basée sur le Cloud a permis à vos employés d'être productifs partout et sur tout appareil. Cela a accentué leur besoin d'accéder de façon fluide aux données d'entreprise pour mener à bien leur travail.

Les modèles de sécurité traditionnels consistent à partir du principe que chaque utilisateur et appareil du réseau est digne de confiance, mais cela met votre infrastructure en danger. Dès qu'un utilisateur pénètre dans votre périmètre, il dispose d'un accès quasiment illimité à tout. Cela signifie que vos données sont vulnérables face à toute personne en mesure d'obtenir un accès au réseau, au système ou aux applications en question.

Un accès distant sécurisé doit être dynamique

Vos utilisateurs ne sont plus restreints au seul périmètre réseau traditionnel. À l'heure où la plupart de vos données et applications sont dans le Cloud, vos employés peuvent rester productifs en toutes circonstances, indépendamment du réseau ou de l'appareil qu'ils utilisent.

De nombreuses organisations se sont tournées vers des réseaux privés virtuels (VPN) pour permettre le travail à distance, mais cette approche présente un certain nombre de risques. Premièrement, les VPN octroient un accès illimité à toute personne connectée, sans tenir compte du contexte pour savoir quelle personne ou entité demande cet accès.

AVANTAGES

- Contrôles granulaires et contextuels des identités et des accès
- Sécurité et expérience utilisateur similaires pour les applications SaaS, IaaS et sur site
- Contrôle centré sur l'application, limitant l'accès à ceux qui en ont besoin uniquement
- Masquage des applications, empêchant leur divulgation sur l'Internet public
- Sécurité avancée étendue aux applications existantes grâce à la gestion des accès et des identités
- Accès sans agent depuis tout type de terminal

Deuxièmement, ils ne savent pas si l'appareil qui se connecte au réseau est exempt de logiciels malveillants ou si l'utilisateur donne sa véritable identité.

Troisièmement, un VPN peut également octroyer un accès à d'autres appareils connectés au réseau de l'utilisateur qui ne sont généralement pas sous votre contrôle.

Sécurisation des accès avec Lookout Zero Trust Network Access

Lookout Zero Trust Network Access (ZTNA) surveille en continu l'identité des personnes qui demandent un accès à vos applications et comprend ce dont elles ont besoin pour travailler. Ces informations permettent d'adopter une approche Zero Trust, en fournissant une identité dynamique et un accès contextuel aux données en fonction du niveau de risque que présentent l'utilisateur et l'appareil.

Des politiques d'accès contextuel au niveau de l'utilisateur et de l'appareil

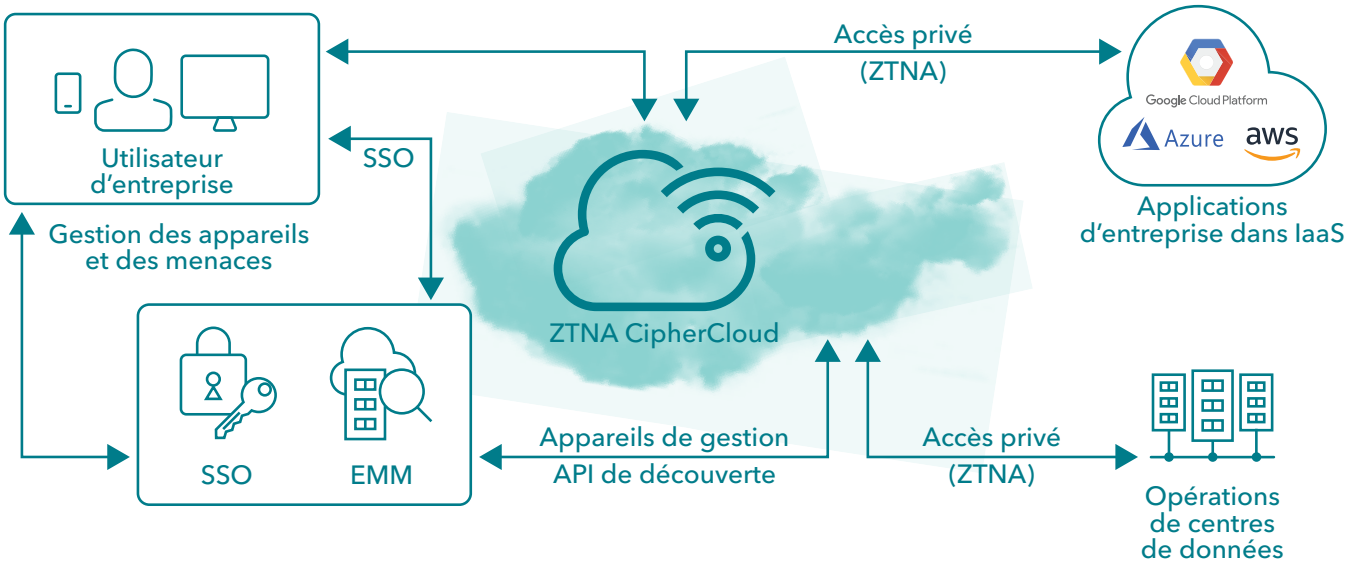
Nous agissons sur le comportement de l'appareil et de l'utilisateur indépendamment l'un de l'autre de façon à créer des politiques contextuelles plus granulaires. Ainsi, les administrateurs réduisent les risques de sécurité associés aux appareils et aux comptes compromis.

Sécurisez vos applications existantes avec des outils basés sur le Cloud

Nous invoquons les mêmes avantages de sécurité d'authentification forte associés aux applications SaaS et aux services Web pour les applications existantes, IaaS et privées. Lookout ZTNA s'intègre à l'authentification à plusieurs facteurs et aux solutions d'identité afin de réduire les contraintes pour l'utilisateur et d'améliorer les contrôles d'accès globaux.

Isolez l'accès applicatif de l'accès réseau avec la micro-segmentation

Lookout ZTNA atténue le risque de violations engendrées par l'octroi excessif de droits d'accès aux différents services. En outre, la solution empêche les acteurs malveillants de s'introduire dans votre infrastructure et de se déplacer latéralement pour dérober plus de données.



À propos de Lookout

Lookout est une entreprise de sécurité cconcentrée sur la sécurité des données utilisées sur les terminaux mobiles ou sur les plateformes Cloud. Notre mission est de sécuriser et développer notre avenir numérique dans un monde où la confidentialité est primordiale et où la mobilité et le Cloud jouent un rôle clé dans notre travail et notre divertissement. Nous permettons aux consommateurs et aux employés de protéger leurs données et de rester connectés en toute sécurité sans porter atteinte à leur vie privée. Des millions de particuliers, de multinationales, d'organismes gouvernementaux et de partenaires font confiance à Lookout, notamment AT&T, Verizon, Vodafone, Microsoft, Google et Apple. 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, rendez-vous sur **www.lookout.com/fr** et suivez Lookout sur son **blog**, sur **LinkedIn** et sur **Twitter**.

Pour en savoir plus, rendez-vous sur
lookout.com/fr

Demandez une démo sur
lookout.com/fr/info/fr-enterprise-contact-us

Sécurité intégrée du terminal au Cloud

Obtenez plus d'informations sur **lookout.com/fr**

Lookout®