Lookout®

LIVRE BLANC

Comment faire confiance à vos terminaux mobiles dans un monde Zero-Trust ?

Les entreprises doivent prendre en compte les 3 affirmations clés suivantes pour protéger leurs ressources contre toute fuite de données et attaque informatique :

1. Le périmètre de votre sécurité s'est estompé.
2. Les technologies de sécurité existantes ne sont pas adaptées.
3. Aucun terminal mobile n'est digne de confiance.

Étant donné que les employés continuent d'utiliser indifféremment des appareils mobiles gérés et non gérés, l'installation d'une nouvelle architecture de sécurité s'impose. **La sécurité extra-périmétrique.**

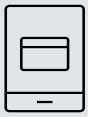
PROBLÈME : Votre périmètre a changé

Les méthodes de travail ont considérablement changé. Les données stratégiques sont désormais disponibles sur le Cloud et les employés peuvent y accéder depuis n'importe quel réseau et où qu'ils se trouvent dans le monde. Par exemple, les employés se connectent très rarement à un VPN pour consulter leurs e-mails professionnels ou pour afficher/télécharger des documents sensibles lors de leurs déplacements.

> **« Gartner prévoit que 80 % des employés travailleront sur un appareil mobile d'ici 2020. »**
>
> - Gartner, « Prepare for Unified Endpoint Management to Displace MDM and CMT », juin 2018

Les attaques, telles que le phishing, ont également évolué et profitent désormais du fait que la sécurité des terminaux mobiles n'est plus assurée. De même, les appareils appartenant à l'entreprise sont désormais utilisés à des fins personnelles. C'est la raison pour laquelle, les applications de réseaux sociaux, de messagerie et autres créent un environnement dans lequel les employés peuvent être la cible de tentatives de phishing et de vol d'identifiants professionnels. Depuis le début de l'année 2018, 50.8 % des utilisateurs de Lookout ayant activé la fonction Safe Browsing ont été victime d'une tentative de phishing.

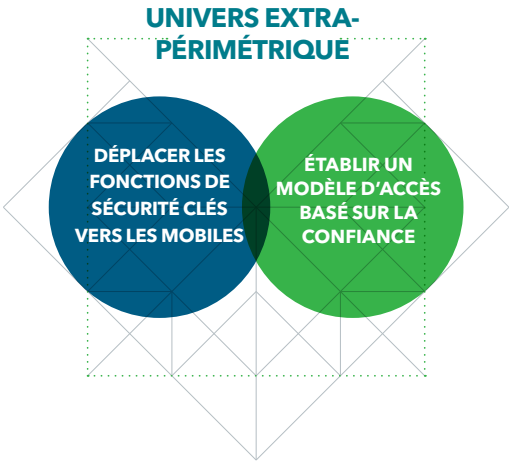
50,8 %



des utilisateurs de Lookout ayant activé la fonction Safe Browsing ont été victimes d'une tentative de phishing en 2018.

La mobilité et l'accès direct à des données sont un véritable atout pour la productivité des entreprises, au plus grand désarroi des équipes chargées de la sécurité, qui ne jurent que par les dispositifs existants au sein du périmètre de leur entreprise, tels que les pare-feux et les passerelles Web sécurisées.

En réalité, les données des entreprises sont de plus en plus en mouvement. Elles sont devenues fluides, mobiles et accessibles. Cette révolution de l'écosystème a fait apparaître deux nouveaux besoins en matière de sécurité :



Déplacer les fonctions de sécurité clés vers les terminaux

Tout d'abord, au lieu de cacher les périphériques derrière le système de sécurité périmétrique, la sécurité doit être déplacée sur le terminal car c'est lui qui accède aux données. Il est inutile de placer des gardes devant votre château s'il n'a plus de muraille... La sécurité doit suivre les données, où qu'elles se trouvent.

Établir un modèle d'accès Zero-Trust

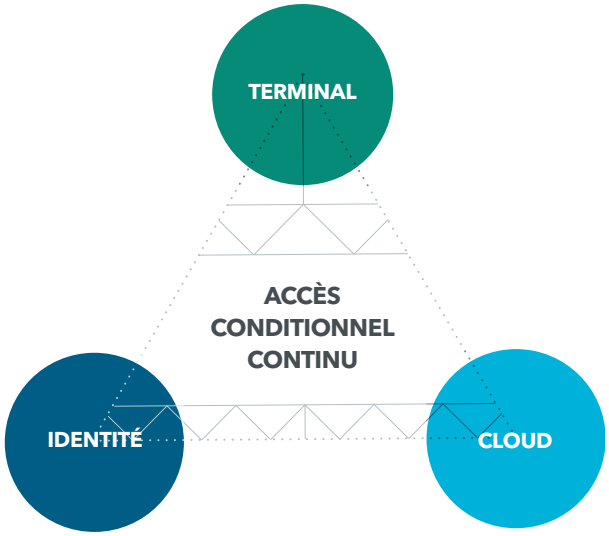
Même lorsqu'un système de sécurité se trouve sur un terminal, la présomption d'innocence est un principe qui ne doit en aucun cas s'appliquer à un poste de travail ou un mobile. Ce nouveau monde implique que la sécurité de tous les appareils soit régulièrement contrôlée pour pouvoir accéder aux données d'une entreprise.

« Zero-Trust : cette expression a été popularisée par l'étude de Forrester, publiée en 2013 pour NIST et intitulée Developing a Framework to Improve Critical Infrastructure Cybersecurity. Cette étude était elle-même inspirée de travaux plus anciens portant sur la dépérimetrisation, menée par l'organisation Jerricho Forum début 2004.»

LA NOUVELLE ARCHITECTURE DE SÉCURITÉ : la sécurité extra-périmétrique

En réalité, les entreprises ont besoin d'un nouveau modèle d'architecture de sécurité appelé « sécurité extra-périmétrique ». À la base, elle se compose de trois pièces de puzzle différentes, mais assemblées les unes aux autres :

- Protection des terminaux
- Accès au Cloud
- Identité



L'architecture de la sécurité extra-périmétrique repose sur l'évaluation des risques d'un appareil à l'aide d'une solution de sécurité. Cette protection permet d'identifier de manière constante les menaces et les risques pesant sur un appareil. La solution détermine ensuite si l'appareil d'un employé est suffisamment sécurisé pour l'autoriser à s'authentifier et à accéder aux ressources de l'entreprise. Grâce à cette protection, une entreprise peut alors appliquer en temps réel des politiques en fonction de sa tolérance face à des risques spécifiques.

Cette architecture repose également sur la protection de l'accès au Cloud d'entreprise, et à Internet dans son ensemble, sans avoir recours aux dispositifs de défense traditionnels (pare-feux, proxys, etc.). Pour que cela soit possible, certaines fonctions de sécurité critiques doivent être déplacées vers le terminal de l'utilisateur ainsi que la surveillance des sites malveillants et, par conséquent, la protection des employés en empêchant tout accès à des contenus à risques.

Ces deux aspects vont de pair avec une solution d'identification, telle qu'un fournisseur SSO (Single Sign-on), pour autoriser un employé à s'authentifier et à accéder aux ressources de son entreprise ou, au contraire, lui refuser le droit de s'authentifier. Une fois l'employé authentifié, le risque associé au terminal sera évalué en permanence et son accès révoqué dès qu'un risque sera détecté. Dans certains scénarios, l'accès aux ressources peut être géré via une solution EMM (Enterprise Mobility Management - pour les terminaux gérés par l'entreprise) ou via une solution MAM (Mobile Application Management - pour les terminaux non gérés).

Accès conditionnel continu

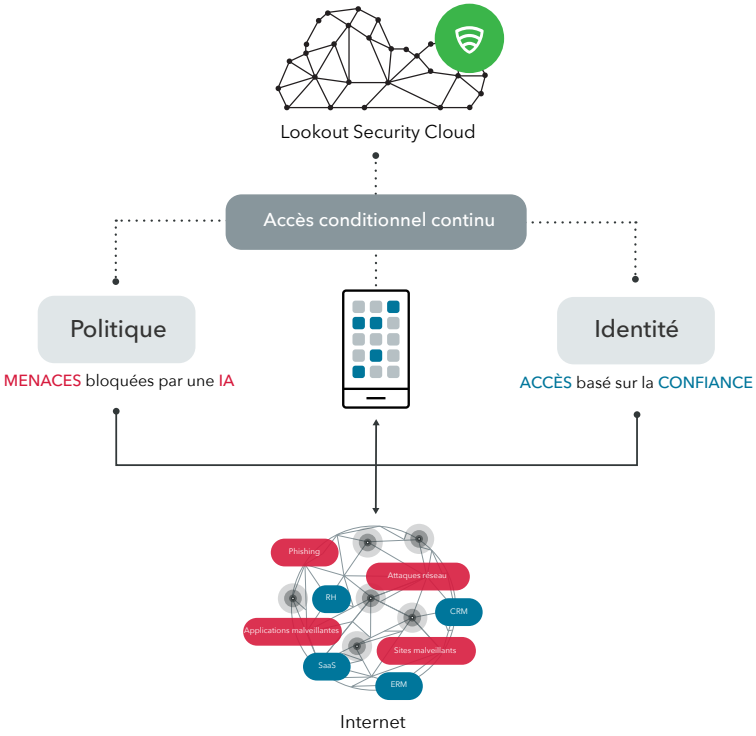
Il s'agit ici d'évaluer les risques afin de contrôler l'accès aux ressources, on parle alors d'« Accès Conditionnel Continu ».

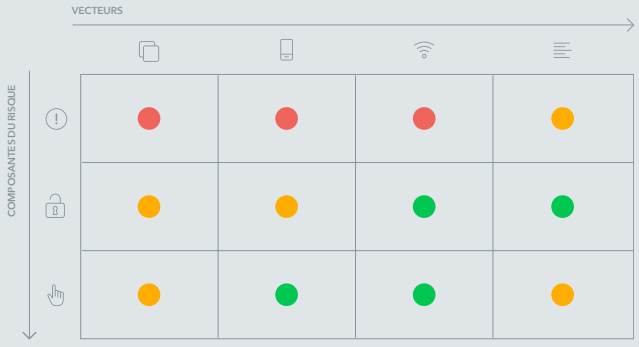
En regroupant les trois principes de base de la sécurité extra-périmétrique, ils veilleront à toujours maintenir les niveaux de risques de votre entreprise au plus bas. En cas de risques avéré, tout accès sera refusé et les ressources de votre entreprise seront donc protégées.

SOLUTION : comment Lookout vous aide à appliquer une solution de sécurité extra-périmétrique

Lookout a spécialement conçu notre plateforme pour permettre aux entreprises d'intégrer concrètement la sécurité extra-périmétrique à leurs effectifs.

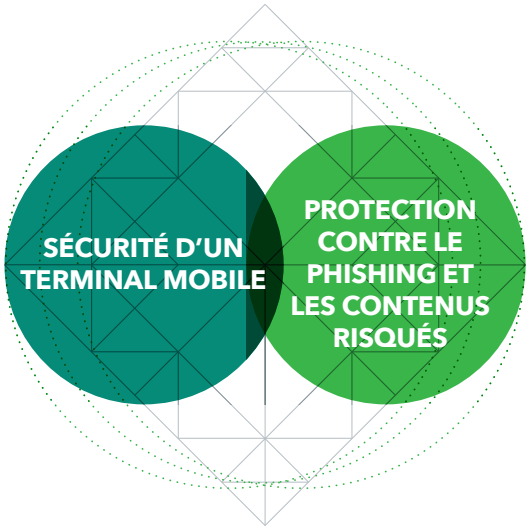
Elle commence par recueillir nos ensembles de données télémétriques de sécurité dans plus de 170 millions d'appareils et 70 millions d'applications dans le monde, Nous fournissons ainsi une quantité d'informations détaillées et inégalées dans le spectre des risques, notamment les menaces et risques pesant sur les appareils, le réseau, les applications et les contenus. Ces informations nous permettent ainsi d'aider les entreprises à identifier immédiatement tout scénario dangereux susceptible de se produire à tout moment sur les appareils des employés.





Le spectre des risques mobiles concerne toutes les entreprises. Découvrez ce qu'il renferme et comment utiliser la matrice des risques mobiles pour connaître le niveau de tolérance aux risques de votre entreprise.

EN SAVOIR PLUS



Via la solution Mobile Endpoint Security

Grâce à Lookout Mobile Endpoint Security, les entreprises peuvent permettre un accès conditionnel continu aux données d'entreprise, depuis n'importe quel appareil. Ce déploiement garantit non seulement l'application permanente de politiques et la validation de la sécurité des appareils avant que les employés ne s'authentifient, mais également une fois qu'ils accèdent aux ressources de l'entreprise.

Les entreprises peuvent sélectionner, selon leur niveau de tolérance face aux risques, des politiques permettant de s'assurer que les appareils restent conformes à leurs exigences internes et externes. Si un appareil dépasse le niveau acceptable de risque de l'entreprise, Lookout enverra un message de correction à l'utilisateur, informera l'administrateur du problème dans la console Lookout Mobile Endpoint Security et déconnectera l'utilisateur qui ne pourra plus accéder à aucune ressource de l'entreprise.

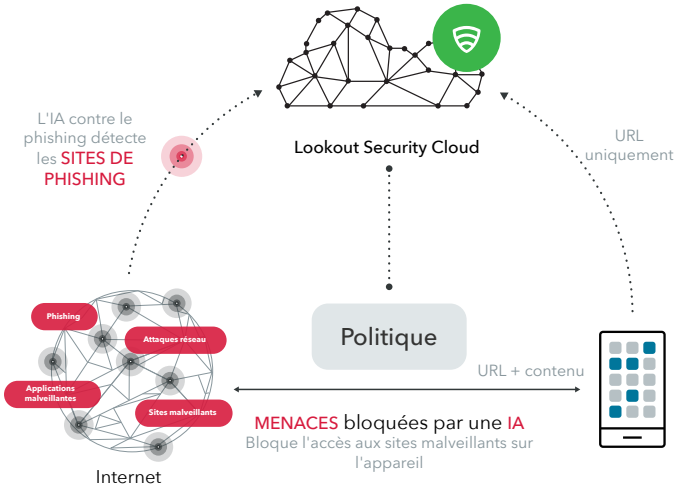
Ce n'est que lorsque l'appareil reviendra à un niveau de risque acceptable, généralement grâce à une action correctrice de l'employé, que ce dernier sera autorisé à s'authentifier pour accéder de nouveau aux ressources de l'entreprise.

Dans la mesure où l'appareil reste en bonne santé, les employés pourront librement accéder aux ressources de leur entreprise.

Via la protection des contenus malveillant et contre le phishing

Pour atténuer les risques de phishing, les entreprises se reposent généralement sur leur solution de sécurité pour la messagerie électronique et leurs passerelles disponibles à l'intérieur de leur périmètre. Bien que la sécurité des e-mails ait toujours sa place dans l'architecture de sécurité moderne, un problème persiste encore. Étant donné que les employés accèdent à des données via des applications autres que celles de messagerie électronique sur des appareils qu'ils utilisent hors du périmètre de leur entreprise, ces technologies sont donc devenues insuffisantes.

C'est l'une des principales raisons pour laquelle la sécurité doit être déplacée sur le terminal. La protection des contenus malveillants et contre le phishing de Lookout est présente sur leurs appareils et surveille toute attaque de phishing sur plusieurs vecteurs différents, notamment les applications de réseaux sociaux, de messagerie, de SMS, et de toute application capable de se connecter à un réseau.



Le moteur de détection reposant sur l'intelligence artificielle de Lookout détermine de manière proactive la réputation des sites Internet. Grâce à son approche continue, l'intelligence artificielle contre le phishing de Lookout détecte les kits de phishing dès leur conception, avant qu'un utilisateur ne soit ciblé et qu'une attaque ne soit exécutée. Nous vous faisons part de certains résultats ici @PhishingAI.

« Nous considérons la sécurisation des téléphones mobiles comme une priorité absolue. Lookout nous sert de couche de protection stratégique, non seulement pour éviter que les données de notre entreprise ne soient compromises, mais aussi pour veiller à leur conformité avec les lois relatives au respect de la vie privée. »

Christian Jösch, administrateur réseau, Simon-Hegele

Le phishing par mobile en 2018 : mythes et réalité dans les entreprises d'aujourd'hui

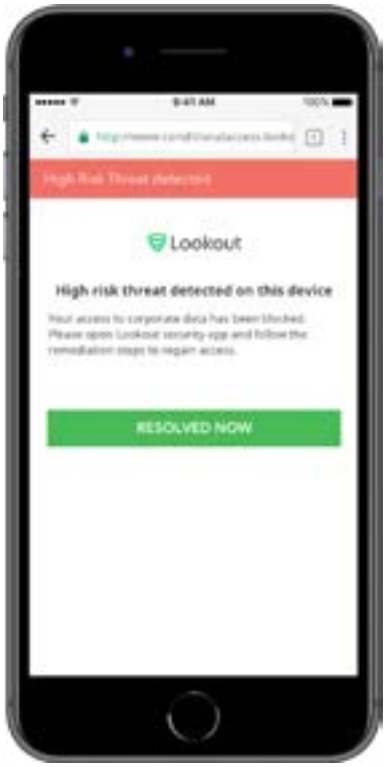
TÉLÉCHARGER LE RAPPORT

RÉSULTATS :
qu'il soit géré ou non, le mobile est sécurisé

Notre façon de travailler a évolué. D'après l'IDC (International Data Corporation), « le pourcentage d'employés considérés «nomades» par les grandes entreprises devrait passer de 35 % aujourd'hui à 43 % dans les 12 à 18 mois prochains. »[1]

Les méthodes de stockage de données, les modes de déplacement des employés, les innombrables appareils se connectant aux ressources des entreprises... tous ces facteurs contribuent à la révolution numérique que les entreprises doivent prendre en compte pour rester compétitives. Très vite, l'expression « endpoint » s'est imposée pour désigner tout appareil qu'utilise un employé pour son travail.

La notion de périmètre, telle que nous la connaissons, a disparu. Les technologies de sécurité existantes sont devenues obsolètes. Les appareils mêmes ne sont pas dignes de confiance, mais il est possible de sécuriser les ressources des entreprises malgré cette nouvelle fluidité des données. La sécurité extra-périmétrique est l'architecture centrale recommandée pour ce nouveau monde du travail.



[1] Source : IDC, The State of Mobile Enterprise Devices in 2018: An IDC Survey of Devices, Decisions, and Deployments, forthcoming, octobre 2018