Étude de cas

Un leader mondial de l'industrie pharmaceutique protège ses recherches avec Lookout

Le challenge

L'une des plus grandes entreprises pharmaceutiques au monde souhaitait prévenir les fuites de données relatives à la propriété intellectuelle. Elle souhaitait également répondre aux exigences de conformité des appareils mobiles utilisés pour accéder aux données de recherche de l'entreprise. Le RSSI de cette dernière a identifié une faille dans sa capacité à se protéger contre les risques de phishing mobile et les risques liés aux applications qui pourraient conduire à une fuite de données pour plus de 20 000 utilisateurs d'appareils mobiles.

Alors qu'un budget avait été alloué à la sécurité mobile, il incombait à l'équipe informatique de gérer le déploiement de toute nouvelle solution. Pour limiter l'impact sur les recherches en cours sur les vaccins, il était essentiel de minimiser les perturbations pendant le processus de déploiement sur l'ensemble de la flotte mobile.

La prise en charge des appareils personnels utilisés pour le travail est omniprésente dans tous les secteurs, y compris l'industrie pharmaceutique. Cela crée un risque important lorsque les appareils personnels accèdent aux données de recherche. C'est pourquoi le RSSI en question s'est rendu compte que, pour sécuriser les appareils personnels, l'organisation devait adopter une approche zero trust. Seuls les appareils personnels respectant les exigences clés en matière de conformité et de sécurité pouvaient accéder aux données. Le défi consistait à appliquer un modèle de zero trust aux terminaux et à faire respecter les exigences de sécurité de manière continue.

Profil du client

Secteur d'activité : Pharmaceutique

Appareils mobiles de soins de santé : 20,000

Politique de mobilité :
BYOD (Bring-your-own-device)

Solution de gestion de la mobilité d'entreprise :
Microsoft Endpoint Manager

Solution de sécurité :
Lookout Cloud Security Platform

Solutions intégrées

Integrated Microsoft Endpoint Manager

Lookout Mobile Endpoint Security

Lookout Phishing and Content Protection

Résultats

- Prévention des attaques de phishing mobile sur les applications professionnelles et personnelles
- Visibilité en temps réel des risques liés aux appareils mobiles
- Activation des politiques d'accès conditionnel pour restreindre l'accès aux données jusqu'à ce que les menaces mobiles soient éliminées
- Sécurisation des terminaux mobiles avec un point de vue unique
- Mise en œuvre des politiques de mobilité BYOD avec Lookout pour la sécurisation de tous les appareils non gérés

Une fois déployée, la solution de sécurité des terminaux mobiles sélectionnée devait protéger contre :

- les attaques de phishing mobile sur toutes les applications, et non pas seulement sur les e-mails
- les logiciels malveillants iOS et Android sur les appareils appartenant aux employés
- les attaques sur des réseaux Wi-Fi compromis ou non sécurisés
- les applications susceptibles de divulguer les données et de compromettre la conformité de l'organisation.

La solution

Après avoir évalué une liste de solutions de sécurité mobile, le RSSI de cette entreprise est arrivé à la conclusion que l'intégration entre Microsoft Endpoint Manager et Lookout Mobile Endpoint Security était la meilleure solution possible. L'intégration fournit la possibilité d'adapter en permanence les contrôles d'accès aux appareils mobiles BYOD en fonction des changements en temps réel du niveau de risque des appareils. Si le niveau de risque devient inacceptable, l'accès peut être automatiquement modifié pour protéger la propriété intellectuelle de l'organisation.

Lookout permet cet accès basé sur le niveau de risque en fournissant une visibilité en temps réel des risques mobiles au gestionnaire des terminaux, ce qui permet une stratégie zero trust pour les utilisateurs d'appareils mobiles. Grâce à une surveillance continue des risques tels que les menaces mobiles avancées, les fuites de données d'applications et les réseaux Wi-Fi compromis, Lookout permet de limiter l'accès aux appareils mobiles compromis. Par exemple, si un employé du département de recherche télécharge à son insu une application mobile malveillante, Lookout identifiera la menace et déclenchera des politiques d'accès conditionnel pour restreindre l'accès aux données de l'entreprise jusqu'à ce que la menace soit supprimée du terminal.

Le RSSI et le DSI ont convenu que les solutions combinées de Lookout et de Microsoft offraient sécurité mobile et zero trust étaient toutes deux nécessaires à la protection de leur propriété intellectuelle. En outre, ils ont réalisé que la gestion de la mobilité d'entreprise (EMM) à elle seule était insuffisante.

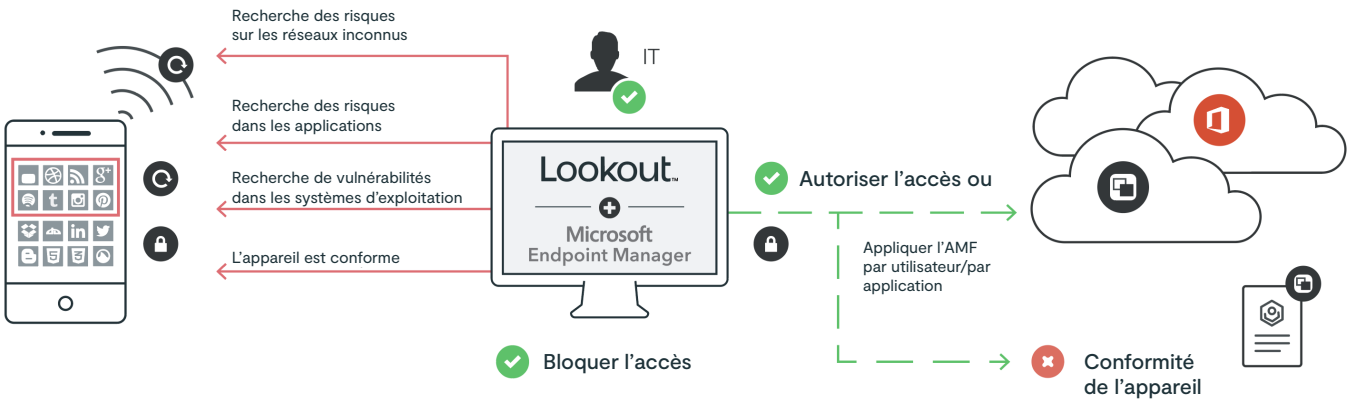
Les politiques de Lookout fournissent une détection des menaces mobiles et une évaluation des risques en temps réel, alors que l'EMM ne vérifie les appareils qu'une fois toutes les deux heures. Avec Lookout, le DSI a pu mettre en œuvre une gestion intégrée des politiques pour les utilisateurs et les groupes et le RSSI a accès en un clic aux rapports de risque et de conformité pour tous les utilisateurs et les applications installées sur leurs appareils.

Resultats

Grâce au déploiement fluide de Lookout, ce géant pharmaceutique est en mesure d'établir une politique de sécurité globale pour ses employés. Si un appareil mobile est jugé non conforme en raison d'un risque mobile, l'accès de l'utilisateur aux ressources de l'entreprise est bloqué. Il ne retrouvera l'accès que lorsqu'il aura résolu le problème en suivant les instructions de remédiation de Lookout.

Depuis que Lookout Mobile Endpoint Security with Phishing and Content Protection s'est intégré à la solution Microsoft EMM, l'organisation est en mesure de tout gérer à partir d'une "vue unique".

Le RSSI et le DSI de cette entreprise pharmaceutique de renom sont désormais en mesure de répondre aux exigences du PDG et du conseil d'administration en matière de protection des terminaux contre les attaques de cybersécurité et de réduire de manière mesurable les risques liés à la mobilité au sein de leurs effectifs internationaux.



À propos de Lookout

Lookout, Inc. est une société de sécurité des terminaux au cloud conçue spécialement pour le croisement des données d'entreprise et des données personnelles. Nous protégeons les données sur les appareils, les applications, les réseaux et le cloud grâce à notre plateforme de sécurité unifiée, cloud-native et aussi fluide et flexible que le monde numérique moderne. En donnant aux organisations et aux individus un plus grand contrôle sur leurs données, nous leur permettons de révéler leur potentiel et de réussir . Des entreprises de toutes tailles, des organismes gouvernementaux et des millions de consommateurs font confiance à Lookout pour protéger leurs données sensibles, leur permettant ainsi de vivre, de travailler et de se connecter librement et en toute sécurité. Pour en savoir plus sur Lookout Cloud Security Platform, visitez fr.lookout.com et suivez-nous sur notre blog, LinkedIn et Twitter.

Pour plus d'informations, rendez-vous sur fr.lookout.com

Demandez une démo sur lookout.com/request-a-demo