Une entreprise de services financiers du classement Fortune 500 corrige une faille de sécurité mobile avec Lookout

Le défi

Une entreprise internationale de services financiers, qui gérait jusque ici les appareils mobiles de ses employés avec une solution EMM, a réalisé qu'elle devait améliorer la visibilité sur la sécurité et la gestion des risques sur ces points de terminaison. Dans le cadre d'une initiative menée par son Vice-président de l'ingénierie mobile, l'entreprise s'est mise en quête d'une solution de sécurité mobile pour relever les défis suivants :

Défis de la sécurité

- Bénéficier d'une visibilité sur les menaces applicatives et inhérentes aux appareils, telles que les applications sideloadées sur iOS et les appareils rootés sur Android
- Atteindre un objectif de conformité imposé en interne pour protéger les données sur les points de terminaison mobiles
- Réduire les risques de fuite de données client, les appareils mobiles étant désormais les points de terminaison privilégiés pour accéder à ce type d'information

C'est en discutant avec de nombreux architectes sécurité et responsables mobilité du classement Fortune 500 dans divers secteurs que nous nous sommes rendu compte que beaucoup d'entreprises rencontraient les mêmes problèmes avec les smartphones et tablettes, deux outils aujourd'hui essentiels aux employés.

Profil du client

Une grande entreprise de services financiers implantée à New York qui exerce ses activités dans plus de 100 pays

Secteur d'activité : services financiers

Politique de mobilité : COPE & BYOD

Solution EMM : MobileIron

La solution

Lookout Mobile Endpoint Security

Les résultats

- L'entreprise a corrigé une faille importante dans sa stratégie de protection des données mobiles
- L'entreprise a démontré la réduction significative des risques aux acteurs internes à l'aide d'un rapport sur les incidents de sécurité détectés et résolus par Lookout
- Lookout Mobile Endpoint Security a permis à cette entreprise du Fortune 500 d'offrir une mobilité sécurisée à ses effectifs internationaux

Les critères

Cette entreprise de services financiers avait besoin d'une solution de sécurité mobile répondant aux critères suivants.

Critères de la solution :

- Une protection multiplateforme solide pour les appareils iOS et Android contre les menaces applicatives et inhérentes aux appareils
- L'intégration aux fonctionnalités de provisioning et de correction des appareils fournies par MobileIron afin de tirer parti des investissements existants de la société dans sa solution EMM

Avec les milliers d'appareils iOS et Android utilisés par ses employés dans le monde entier et une politique de mobilité BYOD, le client était également à la recherche d'un fournisseur de sécurité capable d'offrir une assistance mondiale et une solution adaptée aux appareils personnels des employés.

Le choix de Lookout

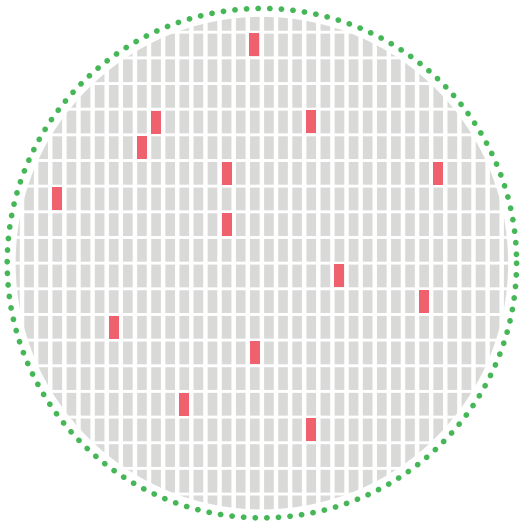
Après s'être renseignée sur un certain nombre de solutions de sécurité mobile, l'entreprise a choisi Lookout Mobile Endpoint Security pour ses capacités de défense optimales, reposant sur un réseau international de plus de 150 millions de capteurs qui lui permet de recueillir des renseignements en matière de sécurité.

Partenaire officiel de détection des menaces de MobileIron, Lookout s'est également intégré à l'actuel fournisseur EMM de l'entreprise, lui permettant ainsi de fournir automatiquement l'application de sécurisation de Lookout à ses effectifs internationaux et de développer des politiques de correction des appareils personnalisées basées sur les renseignements de sécurité et les détections de menaces transmises par le client de point de terminaison de Lookout.

Une réduction significative des risques

Dans les semaines qui ont suivi le déploiement de Lookout sur des milliers d'appareils, le client a constaté une réduction considérable des risques en analysant les incidents de sécurité mobile détectés par Lookout, qui ont, le plus souvent, été corrigés par les employés eux-mêmes.

Les objectifs de l'entreprise	Les résultats obtenus avec Lookout
Bénéficier d'une visibilité sur les menaces applicatives et inhérentes aux appareils	La console de Lookout offre aux administrateurs une visibilité en temps réel sur les menaces applicatives et inhérentes aux appareils dans le parc mobile
Respecter les exigences internes en matière de conformité des points de terminaison	Lookout Mobile Endpoint Security agit comme un contrôle technique pour protéger les points de terminaison mobiles
Réduire les risques de fuite de données client	Lookout détecte et corrige les menaces mobiles, telles que XcodeGhost, qui pourraient entraîner des fuites de données client



Détections sur 30 jours de déploiement (7 700 appareils)

iOS	**Applications sideloadées**	
	110 détections d'applications sideloadées	Les applications sideloadées ne sont pas examinées par Apple et peuvent fonctionner sur des appareils iOS non-jailbreakés, car elles utilisent des certificats de provisionnement d'entreprise. Elles présentent donc un risque de sécurité potentiel et peuvent être un vecteur de logiciels malveillants susceptibles de voler des données d'entreprise si les attaquants compromettent un certificat de provisionnement d'entreprise ou s'ils l'obtiennent frauduleusement de toute autre manière.
	Chevaux de Troie	
	1 détection (XcodeGhost) 1 détection (YiSpecter)	XcodeGhost, un cheval de Troie qui vole les données des appareils affectés, a été inséré dans un certain nombre d'applications iOS dans l'App Store via une version compromise de Xcode, l'outil de développement d'Apple. Cette menace peut être utilisée pour récupérer les informations de connexion des utilisateurs finaux en les invitant à visiter des pages Web frauduleuses. YiSpecter est un cheval de Troie qui peut installer et exécuter arbitrairement des applications iOS et voler les données des appareils affectés.

Android	**Appareil compromis**	
	1 détection d'appareil rooté	Le rootage permet aux attaquants potentiels d'obtenir des privilèges d'administration supérieurs et peut compromettre les fonctionnalités de sécurité natives d'Android, comme le cloisonnement par sandbox des applications, ou les fonctionnalités de sécurité qui dépendent du système d'exploitation, comme les conteneurs d'applications.
	Menaces applicatives	
	102 détections de riskware 2 détections de chargeware 7 détections de adware	Les applications riskware comprennent le code, les bibliothèques ou les services réseau qui présentent un risque pour les appareils en raison de vulnérabilités connues ou de la faible fiabilité des fournisseurs de services utilisés par les applications. Les chargewares entraînent une facturation indue sur la facture de téléphone mobile de la victime. Les adwares affichent des publicités intrusives ou envoient des données personnelles potentiellement confidentielles, comme le numéro IMEI, aux réseaux publicitaires, allant au-delà des pratiques publicitaires courantes.

Après avoir implémenté Lookout Mobile Endpoint Security, l'entreprise de services financiers a corrigé une faille importante dans sa stratégie de protection des données mobiles et a atteint ses principaux objectifs opérationnels.

En outre, pendant les semaines qui ont suivi le déploiement de Lookout sur des milliers d'appareils, le Vice-président de l'ingénierie mobile a pu démontrer la réduction significative des risques aux acteurs internes à l'aide d'un rapport sur les incidents de sécurité détectés et résolus par Lookout. En résumé, Lookout Mobile Endpoint Security a permis à cette entreprise du Fortune 500 de mettre en place une mobilité sécurisée pour ses employés dans le monde entier.

Pour obtenir une évaluation gratuite des risques mobiles et mieux comprendre le profil de risque de votre entreprise, contactez-nous à l'adresse lookout.com/fr.