Un grand prestataire de santé déploie Lookout pour protéger ses données sur mobile

Le défi

C'est sur les recommandations d'un récent audit de conformité et afin de protéger les données médicales personnelles et les dossiers médicaux électroniques que le Responsable informatique et l'Architecte sécurité de ce prestataire de santé ont décidé d'ajouter un système de protection à leur flotte d'appareil mobiles. En tant que Responsables de la technologie et de la sécurité, une de leurs priorités est de s'assurer que l'accès aux données des patients, à partir d'appareil mobiles, soit protégé comme le stipule la loi américaine de santé publique HIPAA (Health Insurance Portability and Accountability Act). Ils souhaitaient plus particulièrement protéger les données des menaces applicatives provenant de logiciels malveillants ou de fuites découlant d'applications non conformes.

L'équipe utilisait déjà la fonctionnalité de liste noire de sa solution EMM MobileIron pour empêcher les employés d'utiliser certaines applications sur les appareils iOS de l'entreprise, mais elle a vite réalisé qu'il fallait améliorer le processus manuel de contrôle des applications et les limites de la liste noire, qui ne permet d'ajouter qu'une application à la fois. La liste noire, dont l'opposée est la liste blanche (un système qui permet d'approuver des applications spécifiques), n'est ni efficace ni viable en raison du volume des nouvelles applications et de la fréquence des mises à jour, qui peuvent se produire jusqu'à 26 fois par an. À titre d'exemple, l'application Facebook est mise à jour toutes les deux semaines environ. Contrôler les applications et dresser des listes manuellement nuit à la productivité des employés et ne leur permet pas d'utiliser les applications les plus utiles.

Profil du client

Secteur d'activité : santé

Taille : parmi les 5 premiers systèmes de santé aux États-Unis.

Politique de mobilité : COPE

Solution EMM : MobileIron

Défis de la sécurité

- Adopter les recommandations de l'audit de conformité réglementaire
- Trouver une solution plus rentable que l'ajout manuel des applications à la liste noire
- Obtenir une visibilité détaillée des logiciels malveillants et des points de terminaison mobiles

La solution

Le prestataire de santé a choisi Lookout Mobile Endpoint Security en raison de son excellente capacité à détecter les logiciels malveillants, de la grande visibilité qu'il offre sur le comportement des applications et de l'expérience de l'utilisateur final. Pour la première phase de l'implémentation, nous avons travaillé avec le fournisseur de services informatiques de l'entreprise pour déployer Lookout sur 5 000 appareils iOS gérés utilisés par le personnel de santé et les infirmiers à domicile.

Pour réduire le risque de fuite de données à partir d'applications non malveillantes, l'équipe voulait pouvoir mettre rapidement sur liste noire les applications ayant des comportements incompatibles avec les politiques de conformité. Il s'agissait notamment de définir des politiques personnalisées qui déterminent les applications autorisées en fonction du mode de traitement et de transmission des données sensibles de ces applications.

Avec Lookout, l'équipe peut maintenant définir des politiques personnalisées pour prévenir les fuites potentielles de données des patients. Par exemple, pour éviter la fuite de dossiers de contact des patients protégés par la loi HIPAA, les administrateurs peuvent définir une politique qui empêche les infirmiers à domicile d'utiliser une application capable d'accéder à ces dossiers sur les iPad de l'entreprise.

> « En tant que prestataire de santé, notre priorité est de protéger les données des patients. Cependant, il était difficile d'avoir toutes les informations sur les accès aux données étant donné la quantité d'applications mobiles disponible. Nous avons sélectionné Lookout, car il nous offre la visibilité dont nous avons besoin sur le comportement des applications. Nous n'avons plus à mettre les applications sur liste noire une par une, ce qui représente un vrai gain de temps. »
>
> **Responsable informatique du site**

Les prochaines étapes

Les deux prochaines phases du renforcement de la sécurité mobile de l'entreprise consisteront à travailler avec Lookout pour examiner la sécurité des applications de santé traditionnelles lors de leur portage sur iOS et à déployer Mobile Endpoint Security sur d'autres appareils mobiles.

Les équipes de l'informatique et de la sécurité de ce prestataire de santé de premier plan ont conscience qu'il est essentiel de mettre en place une sécurité mobile complète pour garantir la conformité et éviter la fuite de données.