Buurtzorg protège ses données de santé en sécurisant ses 8 000 iPads

Le défi

Les infirmier(ère)s à domicile de Buurtzorg Nederland (Buurtzorg) passent la plus grande partie de leur temps en déplacement à rendre visite à leurs patients pour leur donner des soins. Ces infirmier(ère)s utilisent des iPads fournis par leur entreprise et équipés de la plateforme de gestion de la mobilité en entreprise (EMM) MobileIron comme principal outil de productivité.

Le parc d'iPads leur permet d'accéder à des informations sensibles sur les patients, y compris des évaluations et des informations de facturation via l'application propriétaire de Buurtzorg. Les infirmier(ière)s utilisent par ailleurs fréquemment des connexions Wi-Fi publiques pour accéder aux applications qui leur servent au quotidien pour différentes tâches, comme évaluer des blessures. Pour la direction de Buurtzorg, ces différentes utilisations n'étaient toutefois pas sans poser problème. Elle souhaitait certes que ses employés puissent utiliser librement leurs iPads de la manière la plus productive possible, mais avait en même temps conscience qu'il fallait établir et gérer des politiques concernant les applications acceptables afin de protéger les données des patients.

> « Mettre des applications sur liste noire est très compliqué, car il y a beaucoup d'applications dans l'App Store et si nous en mettons sur liste blanche, les employés n'ont plus beaucoup de liberté. »
>
> **Jos de Blok**, PDG et cofondateur

BUURTZORG

Profil du client

Buurtzorg Nederland est une société néerlandaise de soins à domicile connue pour ses équipes d'infirmier(ère)s autonomes qui fournissent des soins de qualité. Le nom de la société signifie en français « soins de quartier ».

Secteur d'activité : santé

Politique de mobilité : COPE

La solution

Lookout Mobile Endpoint Security

Les résultats

- Élimination à 100 % des menaces mobiles, effectuée par des utilisateurs non techniques
- Productivité améliorée pour les équipes d'infirmier(ère)s à distance
- Mise en conformité avec les lois néerlandaises sur le respect de la vie privée concernant la sécurité des données privées sur des appareils mobiles
- Visibilité sur le réseau et les menaces applicatives mobiles pouvant entraîner des pertes de données

Défis de la sécurité :

- Permettre à un grand nombre d'employés travaillant à distance de se connecter librement aux réseaux Wi-Fi disponibles sur les sites des clients tout en réduisant le risque d'attaques de type man-in-the-middle
- Se conformer à une loi néerlandaise stipulant que les entreprises doivent faire de leur mieux pour protéger les informations contenues dans les appareils
- Démontrer aux clients que leurs informations personnelles sont en sécurité avec Buurtzorg
- Bénéficier d'une visibilité sur les menaces applicatives et inhérentes aux appareils, telles que les applications sideloadées sur iOS

Fermer complètement l'accès à l'App Store n'aurait pas fonctionné car trop restrictif. La société a également décidé que gérer une liste blanche/noire d'applications ne constituait pas une solution durable. C'est à ce point d'inflexion qu'Ecare TCS, le fournisseur de services gérés de Buurtzorg, a suggéré Lookout Mobile Endpoint Security.

La solution

Pour relever ces défis de la sécurité mobile, Ecare TCS a travaillé avec Buurtzorg afin de déployer et activer Lookout Mobile Endpoint Security sur 8 000 iPads. « Avec la solution Lookout de sécurité mobile d'entreprise mise en place pour détecter les menaces, Buurtzorg peut désormais définir une politique de mobilité qui permet à une équipe d'infirmier(ères) de librement utiliser les connexions Internet et les applications pour fournir de manière efficace des soins de qualité, tout en bénéficiant d'une visibilité complète sur son parc d'iPads », explique Jeffrey Scholten, conseiller informatique chez Ecare TCS.

Ecare TCS et Buurtzorg ont pu facilement déployer l'application Lookout For Work pour un segment d'employés en utilisant MobileIron et en installant l'application à distance sur les appareils, sans aucune intervention des employés. Un autre segment d'employés a quant à lui téléchargé l'application Lookout For Work via un code d'inscription personnel en un clic. Le déploiement s'est déroulé de façon simple et non disruptive pour tous les employés de Buurtzorg, ce qui montre que même des utilisateurs finaux qui ne sont pas nécessairement férus d'informatique peuvent rapidement installer et activer l'application Lookout sur leurs iPads d'entreprise.

Critères de la solution :

- Doit pouvoir protéger les appareils iOS des menaces réseau et applicatives
- Doit s'intégrer 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
- Doit permettre la mise en conformité avec les lois néerlandaises sur le respect de la vie privée obligeant les entreprises à protéger les données sensibles de leurs clients sur les appareils mobiles
- Doit proposer une expérience utilisateur conviviale qui permette aux employés sans connaissances techniques particulières de corriger eux-mêmes toute menace détectée

Les résultats

Lookout Mobile Endpoint Security a détecté un nombre significatif d'attaques de type man-in-the-middle et plusieurs applications sideloadées à risque élevé sur les appareils de Buurtzorg dès les 30 premiers jours qui ont suivi le déploiement.

Lorsqu'une menace est détectée, plusieurs options sont disponibles pour l'éliminer. L'équipe d'Ecare TCS peut soit intervenir directement à travers sa solution EMM MobileIron, soit permettre à l'utilisateur final d'intervenir lui-même sur son propre appareil. Comme les employés de Buurtzorg ont été formés à gérer les menaces mobiles détectées par Lookout, les attaques de type man-in-the-middle ont été neutralisées par les utilisateurs finaux en moins de huit minutes en moyenne. Les détections d'application sideloadée ont quant à elles été gérées par les utilisateurs dans un délai de sept heures en moyenne.

Avec 100 % des menaces mobiles éliminées par des utilisateurs finaux non techniques, Buurtzorg a pu réduire les risques mobiles et permettre à ses équipes d'infirmier(ère)s déjà connues pour leur productivité d'être encore plus performantes. Les employés de Buurtzorg sont désormais libres de télécharger les applications dont ils ont besoin et de se concentrer sur ce qu'ils font le mieux, tout en laissant Lookout Mobile Endpoint Security garantir la sécurité de leurs appareils et des données privées de leurs patients.

L'entreprise a ainsi pu réaliser chacun des objectifs définis lorsqu'elle a lancé son initiative de sécurité mobile, à savoir fournir une mobilité sécurisée, se mettre en conformité avec les lois sur la protection de la vie privée et bénéficier d'une visibilité totale sur les menaces mobiles.