Buurtzorg protects healthcare data by securing 8K iPads

The Challenge

Buurtzorg Nederland (Buurtzorg) home care nurses spend the vast majority of their time traveling to visit patients and serving them in their homes. These nurses use company-owned iPads, managed with MobileIron Enterprise Mobility Management (EMM), as their main productivity tool.

The fleet of iPads give the nurses access to sensitive patient information such as nursing assessments and billing through Buurtzorg's own app. The caretakers also frequently use public Wi-Fi connections to access apps that assist them in daily tasks like evaluating injuries. These use cases created a challenge for leaders at Buurtzorg. They wanted employees to freely use their iPads in the most productive way, but also felt they had to establish and manage policies for acceptable apps in order to protect patient data.

> "Blacklisting apps is very difficult because there are a lot of apps in the App Store and if we whitelist apps, employees don't have very much freedom anymore."

Jos de Blok, CEO and co-founder

BUURTZORG

Customer Profile

Buurtzorg Nederland is a Dutch home health care organization renowned for its use of self-governing teams of nurses to deliver high-quality care. The company's name is Dutch for "neighborhood care."

Industry: Healthcare

Mobility Policy: COPE

The Solution

Lookout Mobile Endpoint Security

The Results

- 100% mobile threat remediation, completed by non-technical users
- Improved productivity for remote nurse teams
- Gained compliance with Dutch privacy laws regarding the security of private data on mobile devices
- Achieved visibility into network and app-based mobile threats with the potential to cause data loss

Security Challenges:

- Enable a large, remote workforce to freely connect to available Wi-Fi at client sites while mitigating the risk of man-in-the-middle attacks
- Comply with a Dutch law stating that companies must do their best to protect information on devices
- Demonstrate to clients that their sensitive information is safe with Buurtzorg
- Gain visibility into app- and device-based security threats such as sideloaded apps on iOS devices

Completely closing off access to the App Store wouldn't work because it was too restrictive. The company also decided that managing a white/blacklist of applications wasn't a sustainable solution. It was at this inflection point that Ecare TCS, Buurtzorg's trusted managed-services provider, suggested Lookout Mobile Endpoint Security.

The Solution

To solve its mobile security challenges, Ecare TCS worked with Buurtzorg to deploy and activate Lookout Mobile Endpoint Security on 8,000 iPads. "With the Lookout enterprise mobile security solution in place to detect threats, Buurtzorg is now able to set a mobility policy that allows its nurse teams to freely use internet connections and apps to deliver high-quality care efficiently, while gaining full visibility into threats among their iPad fleet," said Jeffrey Scholten, IT advisor for Ecare TCS.

Ecare TCS and Buurtzorg easily deployed the Lookout For Work app via MobileIron to a segment of employees by pushing the app to the devices without the need for employee action. Another segment of employees downloaded the Lookout For Work app via a one-click personal enrollment code. The roll-out was simple and non-disruptive for all Buurtzorg employees, proving that even non-technical end-users can quickly install and activate the Lookout app on their corporate iPads.

Solution Criteria:

- Must be able to protect iOS devices from network- and app-based threats
- Must integrate with MobileIron's app provisioning and device remediation capabilities to leverage their existing investment in EMM
- Must enable compliance with Dutch privacy laws requiring companies to protect sensitive client data on mobile devices
- Must have a simple user experience that makes it easy for non-technical employees to self-remediate any threat that is detected

The Results

Lookout Mobile Endpoint Security detected a significant number of man-in-the-middle attacks and several high-risk sideloaded apps on Buurtzorg devices within the first 30 days of deployment.

Once a detection occurs there are several options to remediate the threat. The Ecare TCS team could either take action through their MobileIron EMM solution, or enable the end-user to remediate the threat on their own device. Since Buurtzorg employees were educated on how to handle mobile threats detected by Lookout, the man-in-the-middle detections were remediated by end-users in less than eight minutes on average. The sideloaded app detections were also user-remediated after an average of seven hours.

With 100% mobile threat remediation completed by non-technical end-users, Buurtzorg reduced their mobile risk, and enabled their famously productive nurse teams to reach even higher levels of performance. Buurtzorg nurses now have the freedom to download apps they need and can focus on what they do best, while Lookout Mobile Endpoint Security ensures their devices and their clients' private information stays safe.

The company has achieved every one of the goals stated at the beginning of their mobile security initiative by delivering secure mobility, enabling compliance with privacy regulations, and gaining visibility into mobile threats.