How Lookout Protects Employee Location Data

Many apps ask for location data – take back control of employee privacy

Security and Business Challenges

IT and security administrators face new challenges every day as the reliance on mobile grows. As employees leverage more mobile apps for both personal and work reasons, admins need a way to vet each additional app that is introduced into the mobile fleet. By doing so, they can ensure that no apps have access to data that could harm the company if it were to be exposed.

One of the biggest risks is location data. Employees are oftentimes unaware of what apps are tracking their location and where that information is being sent. With the world's largest mobile data set, the Lookout Security Cloud shows that more than 40% of new Android apps in 2019 collected specific user location data.

Industry Challenges

1. Many harmless apps ask for location, which can be dangerous if hacked.
2. Organizations need to understand which data an app can access and where it's being sent.
3. Security teams need a way to easily blacklist apps that access or send data that shouldn't be out in the world.

Location Tracking in the Real World

When the United States Army and Navy decided to ban the popular social media app TikTok because the location data was initially being sent to China, many organizations followed suit. This decision highlights the growing importance of knowing what data is collected by mobile apps, and where that information is shared. Admins must have a comprehensive tool that shows a breakdown of the apps when they're installed and allow IT to make informed decisions the risk it may pose to their organization.

In a recent series on mobile device tracking, New York Times pointed out was able to track the location of one of President Trump's Secret Service agents, which is just as useful to an attacker as tracking the President himself. By the same token, an attacker could track the location of a company's executive team to put together data about where else they may be doing business, what deals could be going on, or where they're conducting product research.

Knowing the location of high-ranking individuals can tell someone a lot about an organization. Location data can give malicious actors the contextual data and clues they need to leverage an opportunity and attack individual employees or the organization as a whole.

Lookout Critical Capability

Employee location, even when anonymized, can give malicious actors insight into the behaviors of your employees. To help protect all your employees, Lookout's mobile app policies allow admins to block the use of specific apps that collect location data. Lookout's App Analysis also provides in-depth data about the app and helps admins make informed decisions based on risk, capabilities, network activity, and permissions.

Why Lookout

Lookout Mobile Endpoint Security ensures security and compliance on every device, leveraging a large data set fed by over 185 million devices and the analysis of over 100 million mobile apps. With the Lookout Security Cloud, it's easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by dynamic device health checks to provide conditional access to sensitive corporate applications and data.