Android 5.1 Gains Business-Friendly Device Protection Feature

Google includes a new mobile device security feature in its latest Android 5.1 Lollipop update to make the operating system more suitable for business use.

By adding a critical new security function to its latest Android 5.1 update to Lollipop, Google is building on efforts to make its mobile operating system more enterprise friendly.

Earlier this year the company launched an Android for Work program that is enabling multiple partners to integrate key enterprise mobility management capabilities into Android.

Under the program Google will deliver device, application and content management tools that make it easier for IT organizations to separate and manage enterprise data and applications running on personally- owned Android smartphones in the workplace.

Monday, Google announced the availability of a new “Device Protection” capability on Android 5.1 that builds on its effort to make Android smartphones a little more business- friendly. The feature is similar to the Activation Lock on the Apple iPhone in the sense that it prevents unauthorized users from using a lost or stolen Android smartphone.

According to Google, with Device Protection, a lost or stolen device will remain locked until the legitimate user signs into the device via their Google account. The device will remain locked even if it has been returned to its original factory settings, Google said. The Device Protection feature will be available on most Android 5.1 smartphones as well as on Nexus 6 and Nexus 9 handsets, the company said.

The lock functionality should help relieve at least some of the concerns that IT administrators might have in allowing employees to use Android devices to access and store business applications and data. For businesses, it reduces the danger of data leaks and data theft resulting from lost or stolen Android devices.

This is the second important security improvement that Google has incorporated directly in to Lollipop in recent months, said Roman Foecki, CEO of security vendor CoSoSys. In November, Google said it would add a default device encryption capability for protecting data stored on Android devices, he noted.

A similar feature has been available to iOS users for some time and shows Google’s commitment to making Android more suitable in the workplace, Foecki said.

“In the coming Android versions, we expect to see more security features to be added to Android directly from Google,” Foecki wrote in an email to *eWEEK*. "The company is working hard to increase its footprint in the high-margin enterprise market that has become more and more dominated by Apple's iOS.”

As a mobile operating system primarily designed for consumer use, Android, until recently lacked functions that are critical for use in the workplace.

For instance, prior to Lollipop, Android offered no easy way for IT administrators to separate business and personal content on employee- owned systems. Similarly, Google has committed to supporting default device encryption on Lollipop, but the company has not yet fully implemented that capability.

Google’s moves to bolster Android’s security capabilities appear to be a bid by the company to stem Apple’s

continued and growing dominance in the enterprise market.

A recent report by Good Technology showed that iOS use is increasing among companies adopting Bring Your Own Device (BYOD) and Corporate-Owned Personally-Enabled (COPE) mobility strategies. In the final quarter of 2014, iOS devices accounted for 73 percent of all mobile devices activations in the enterprise compared to 25 percent for Android.

In regulated industries, iOS had an even bigger share, accounting for 95 percent of all mobile device activations in the legal sector, 82 percent in the public sector and 81 percent among financial services companies, according to the Good Technology report. Android fared better in particular industries such as high-tech, manufacturing and transportation.