A recent research by an enterprise mobile threat protection company called Appthority shows that about 97 percent of apps do not pass Apple’s new mandate for cyber security. With only three percent of apps adhering to the mandate and Apple’s App Transport Security requirement deadline coming nearer, it would not be wrong to say that companies need to work a lot in the security domain to make their apps run successfully in future.

The research studied 200 top rated iOS apps installed on corporate devices all over the world and determined how many of them have already applied ATS and to how much extent the security mandate by Apple has been implemented within those apps.

In a statement, Robbie Forkish, Vice President of Engineering at Appthority said, “Although Apple’s ATS encryption requirements go into effect in just a few weeks, Appthority researchers found that the majority of apps in the enterprise don’t fully utilize the best practices encryption standard, which should be a concern to enterprises.”

He went on to say, “The new ATS mandate only applies to new submissions to the App Store, and Apple will be allowing exceptions to ATS, so while the requirement should strengthen data security, there will still be iOS apps not using data encryption in enterprise environments, even after Jan. 1. For this reason, it’s incredibly important that businesses have visibility into, and management of, the risks related to apps with these exceptions, as they can put enterprise data at risk.”

The research also showed that ATS was not enabled for all networks on 83 percent apps whereas 26 percent apps had disabled ATS all over the world, with domains set up as exceptions. Moreover, 55 percent of apps allowed using HTTP instead of HTTPS. Appthority says that existing apps noncompliant with ATS will not be removed from the App Store. However, new apps and updates to current apps will require mandatory compliance to ATS.