Armour Comms launches secure management of mobile communications on BYOD devices

New Configuration Management System safeguards sensitive conversations and messages and reduces the risk associated with BYOD or locally purchased devices

LONDON, UNITED KINGDOM, September 20, 2022 / EINPresswire.com/ -- Armour Comms is launching its new Configuration Management System at the International Cyber Expo, being held at London Olympia, on 27 and 28 September. The new solution is part of Armour's award-winning secure communications flagship platform, Armour Mobile, and will enable organisations to securely manage risk associated with communications data transmitted over Armour Mobile, even on an unmanaged Bring-Your-Own-Device (BYOD) or locally purchased devices.

> People do not like their personal devices to be subjected to corporate Mobile Device Management (MDM) solutions - the Armour Mobile Configuration Management System addresses this conundrum"
>
> *David Holman, Director, Armour Comms*

David Holman, Director at Armour Comms, stated: "The use of BYOD devices has long been an issue for many organisations, and is particularly pertinent in sectors that require data protection, such as defence, government, finance, legal and healthcare. However, people do not like their personal devices to be subjected to corporate Mobile Device Management (MDM) solutions and organisations are concerned about the legal issues of controlling data on devices not owned by them. The Armour Mobile Configuration Management System successfully addresses this conundrum."

Armour Mobile Configuration Management (CMS) provides authorised administrators with complete control over data held within the Armour ecosystem on the device. This means that the end user can continue to use their phone as they would normally, while all sensitive communications are safely stored within the application's 'container', without the need for a Mobile Device Management (MDM) system. Data held in the Armour container can only be

accessed by the end user via the Armour Mobile app (i.e. it is not accessible to other applications, such as the device's photo gallery).

Advanced features of Armour Mobile CMS include message retention limits where messages and any attachments are deleted automatically when the retention limit is reached– which minimises risk of loss of organisational data and aids internal audit and compliance. This integrates fully with Armour Mobile's existing 'Message Burn' feature, providing additional security and flexibility. CMS also provides remote wipe, whereby Armour data is wiped from a user's device without the need to physically access the device – critical for when people leave the organisation or lose their device.

-ends-

Andreina West
Andmar
+44 1491281297
email us here