Armour Comms announces enterprise scalability for up to 200,000 users with Armour Core v5

Armour Mobile, the NATO-approved WhatsApp replacement, available for large scale users with Kubernetes deployment options

LONDON, UNITED KINGDOM, October 4, 2022 /EINPresswire.com/ -- Armour Comms is now shipping Armour Core v5, which includes Kubernetes capabilities for enterprise-wide deployments. Already in use by strategic Government departments and large organisations, Armour Mobile can now be installed across broad groups of disparate users remotely and at scale. Software updates, patches and the application lifecycle can be managed more easily and quickly, transparently to the end-user.

> When secure products are easy to use and quick to deploy, people are more likely to use them and security is more effective - Armour Core v5 brings enterprise grade scaling for our larger customers ”
>
> *David Holman, Director, Armour Comms*

Armour Core v5 supports the latest requirement from Apple for APNS push notifications, and also push notifications for Bittium Tough Mobile™ 2 series of ruggedised and secure smartphones (subject to Bittium Secure Suite being installed). In addition, Armour Core now utilises NginX, to provide an extra layer of security at Transport Layer Security (TLS) level and simplify interfaces accessing the service; and uses Prometheus to provide extra monitoring options for SIP and XMPP.

David Holman, Director at Armour Comms, stated: “When secure products are easy to use and quick to deploy, people are far more likely to use them, meaning that the security is more effective. With this in mind, Armour Core v5 brings enterprise grade scaling for our larger customers, and for those organisations that wish to use Kubernetes.

“Armour Core also supports our new Configuration Management System which enables organisations to manage Armour on BYOD devices without the need for a Mobile Device

Management (MDM) solution. The IT/Security department are able to manage data, apply updates and wipe Armour data remotely (useful for when someone leaves or a device is lost/stolen), transparently, quickly and with minimal resource overhead."

Armour Mobile Configuration Management (CMS) provides authorised administrators with complete control over data held within the Armour ecosystem on the device. The end user is able to continue using their phone as they would normally, while all sensitive communications are safely stored within the Armour '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.

Andreina West
Andmar
+44 1491 281297
email us here