



The need for Enterprise-grade Secure Comms in today's business world

Messaging apps such as WhatsApp, Telegram, Messenger, Viber and their ilk have taken the world by storm. Free to use, they promise end-to-end encryption and security. They are quick to download and because most people are using them, they can be quite compelling. It was only a matter of time before they were adopted, often by stealth, for corporate communications, even though they are not suitable for business use and in the UK and Europe, they do not meet data regulations such as GDPR.

While some organisations have gone so far as to ban the use of WhatsApp, (<https://www.dw.com/en/germanys-data-chief-tells-ministries-whatsapp-is-a-no-go/a-53474413>) the issue is that once people have experienced the ease of use of these consumer chat apps, it's difficult to stop their use. The alternative is to give people something even better than WhatsApp – secure comms with enterprise-grade features which gives control back to the organisation.

The type of features we mean are:

Full enterprise functionality. Including voice calls, text/chat, video, conferencing and attachments – all of which are managed inside the app, stay inside the app, and are completely encrypted so corporate data remains protected.

A choice of on-premises or cloud hosted instance giving complete control of where your data is stored and who has access to it.

Contact lists or communities that are managed centrally. Only pre-approved users can join a call. Everyone knows exactly who they are communicating with – no spoof users with stolen identities.

No requirement to use a mobile phone number. The ability to use a service without using a mobile phone number is an extra layer of security that can keep business and personal communications separate even on the same device, and which also keeps users' personal details private.

Secure video conferencing enabling professional collaboration with all the features provided by the likes of Team and Zoom, but with the additional facility to see all other users on the call and if someone is using the app, or a browser. This significantly reduces the risk of 'zoom-bombing' and nefarious eavesdroppers.

Scalable, fast provisioning for new users. With the use of secure, one-time use QR codes to get new users up and running with the minimum of fuss. Quick for users, and the IT department.

Professional support services. Both phone and email support.

There is much more to security than encryption

There is so much more to security than merely encryption – as this is rarely the weakest link it is therefore rarely the attack vector – which is why it is critical to provide a fully feature solution that is designed specifically for enterprise use with additional features that secure data and protect privacy at all times.

Additional Information

About David Holman

David Holman, Director and Co-Founder of Armour Communications has held a variety of sales and general management positions within international organisations in the IT and security industry. David has been a Non-Executive Director for a number of start-up companies in the security industry more recently, CEO and co-founder of Becrypt, where he was instrumental in growing the business to £10m revenue and profitability. David has sat on various Government/industry committees including CIPCOG (chaired by the Cabinet Office) to promote the importance of security products.

About Armour Comms

Armour Comms provides market leading technology for encrypted solutions including voice, video, messaging, group messaging, conferencing and data on everyday smartphones, tablets and desktops. Supplying enterprise and government markets with an easy-to-use technology combined with advanced security techniques to deliver secure collaboration solutions.

For more information please visit: www.armourcomms.com