

Armour Comms announces new rapid provisioning functionality for Enterprise roll out of SigNet by Armour

Signal-based secure communications app extends enterprise features to support organisations moving away from WhatsApp



LONDON, OXON, UNITED KINGDOM,
January 26, 2021 /EINPresswire.com/ --
Armour® Comms, the leading provider

of specialist, secure communications solutions, has announced the availability of SigNet by Armour® v2.1, which includes new features designed specifically for enterprises. SigNet by Armour, provides secure voice, video, messaging, group chat, file attachments and MessageBurn (timed messages) with AES-256 bit encryption for iOS and Android devices, and for use with

Windows 10, macOS and Linux. Based on the well respected Signal app, SigNet by Armour provides additional security features such as an on-premises option for total privacy and no auditability (as well as the choice of cloud installation), secure groups and allow listing features, and a much improved, highly intuitive user interface. New with SigNet v2.1 is support for QR codes and deep links for one-click provisioning which streamlines on-boarding new users, and saves time and resource for IT departments.

“

SigNet by Armour has been specifically designed for use by non-regulated organisations that require enterprise-grade secure communications.”

*David Holman, Director,
Armour Comms*

David Holman, Director at [Armour Comms](#) commented; “SigNet by Armour has been specifically designed for use by non-regulated organisations that require enterprise-grade secure communications. SigNet provides a great user experience, with the assurance of absolute privacy for data and meta-data, that stays completely within the control of the enterprise. At a time of heightened concern about new privacy policies of consumer-grade messaging apps SigNet is a better, more secure alternative that is GDPR compliant, specifically designed for professional use.”

SigNet has a range of built-in features ideal for mitigating security threats in an enterprise

environment, such as;

- Centralised control of device access so only authorised users can connect to the secure communications service;
- Files and attachments are kept within the app and therefore remain encrypted at all times, even when stored on the device;
- Management of connectivity between users and groups to provide security segregation within the user space.
- Automatic alert sent to the sender of a message if a screenshot has been taken by the recipient;
- Peer to peer encryption, removing the need for a central key server;
- No recording or auditability.

SigNet by Armour is available as a Software as a Service (SaaS) product hosted on Armour's secure cloud, or as an on-premises installation, and uses a peer-to-peer key management system.

Armour Comms has published a White Paper: Why WhatsApp Is Not Suitable for the Workplace. For a copy please email: andreina@pra-ltd.co.uk, or download from the website: <https://www.armourcomms.com/whatsapp-white-paper-request/>

ends -

For more information please visit: www.armourcomms.com

Follow us on Twitter: <https://twitter.com/ArmourComms>

Join us on LinkedIn: <https://www.linkedin.com/company/armour-communications-ltd/>

Andreina West

PR Artistry

+44 1491 845553

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/535085690>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.