Armour Comms showcases new secure collaborative working solutions with MOD and Bittium at DSEI

DSEI, 14 – 17 September, 2021,
ExCeL, London,
Stand No: H1-450

LONDON, UNITED KINGDOM, September 9, 2021 /EINPresswire.com/ -- Armour Comms will be showcasing several new capabilities of its OFFICIAL-SENSITIVE, NATO approved Armour® Mobile at DSEI, including a technical preview of its secure collaboration solution, Unity by Armour. Other innovations on show will be Armour's work with the Ministry of Defence (MOD) for secure mobile comms which is currently being successfully deployed across several operational areas to replace use of consumer grade apps; and Armour's unique technology for Bittium devices, which enables users of Bittium's Android TM2 solution to communicate without using the public internet.

> "
> Armour Comms solves the conundrum of a secure-by-default comms application that is still easy to use and quick to deploy at scale."
>
> *David Holman, Director, Armour Comms*

Unity by Armour works in conjunction with Armour Mobile extending its secure collaboration capabilities with secure video conferencing calls (pre-defined or on-the-fly), screen sharing and integration with secure chat groups, in addition to the existing one-to-one secure audio and video calling, and interconnectivity with trusted unified communications systems. Unity by Armour provides picture in picture and multiple screens, and offers a familiar video conferencing interface, making it easy and intuitive to use. Unity by Armour is available with a choice of hosting options, including on-premises installation, ensuring that communities are controlled by invitation-only, increasing security and guarding against 'zoom-bombing'.

Armour Comms will also be showcasing the latest innovation for its NATO approved secure communications solution which now includes unique Secure Push technology from Bittium. This feature allows secure and battery efficient signalling of incoming Armour Mobile calls and messages also in classified networks that do not have connectivity to public Internet.

Armour Mobile runs on Bittium's Tough Mobile™ 2 series of ruggedised and secure smartphones ensuring voice and video conversations, and the associated files and attachments, stay completely private, no matter how hostile the environment. In addition, Bittium Secure Suite provides additional capabilities such as mobile VPN, device and application management, remote attestation and other functions.

Aimed at military, defence, law enforcement and government markets worldwide, Bittium and Armour products provide the same user experience as consumer-grade solutions, while keeping both data at rest and data in transit secure at all times.

David Holman, Director at Armour Comms said; "At Armour Comms we are focused on delivering highly capable, easy to use, intuitive solutions that are robustly secure and suitable for deployment at scale. For specific markets, like Defence we also work closely with our partners to enable higher assurance communications solutions.

"The new capabilities we have on show at DSEI are driven by our users and are designed with the user in mind. Delivering solutions that are easy and pleasurable to use encourages strong user adoption, avoiding the kind of workarounds that often beset traditional secure communications solutions, such as people resorting to the use of highly insecure consumer-grade apps on 'shadow IT' devices. Armour Comms solves the conundrum of a secure-by-default comms application that is still easy to use and quick to deploy at scale."

Armour has recently announced the availability of its Armour Core v4 server-side software which includes a range of enhancements designed to significantly improve performance and usability including support for IPv6, the latest network communications protocol, enabling calls to seamlessly transition between modern networks.

More information about Armour Communications solutions can be found at www.armourcomms.com.

-ends-

Andreina West
PR Artistry
+44 1491 845553
email us here

in today's world. Please see our Editorial Guidelines for more information.