

Secure Communication Solutions

A powerful platform that protects your calls, instant messaging, and conferencing communications. Built for any size of organisation



"An organisation's ability to respond to a breach is severely diminished if its communications are compromised as part of a larger attack."



National Cyber
Security Centre

Based on NCSC's 7 Principles of Secure Communications

In today's world the cyber threat from nation states and cybercriminals to military, government and corporate communications channels is significant and growing. Organisations of every size need to protect their sensitive conversations and messaging with secure endpoint communications solutions strong enough to ensure these channels and related data remain protected, resilient and meet data sovereignty and compliance requirements.

This is where Armour Comms can help. Our secure communications platform manages and protects your information by encrypting voice, messaging and conferencing data and communications with high assurance solutions which can capture, archive and audit data to ensure you remain compliant.

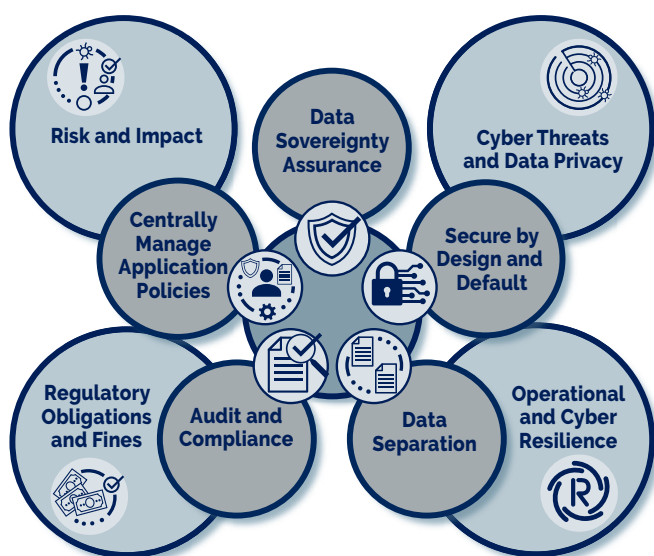
Our solutions are designed to be simple to use, easy to deploy and manage on mobile, desktop and tablet devices. We put the trust back into your communications.

Our platform is suitable for both government and enterprise use, with a range of solutions to address the needs of different use cases, supporting business resilience, regulatory compliance and protecting your data on the end point.

Armour® solutions are approved for use at Corporate Confidential, OFFICIAL-SENSITIVE, NATO RESTRICTED, and SECRET.

Explore the Advantages

How does securing your communications benefit your organisation?



- **Enable Secure Productivity** - Empower your employees to be productive from any location, with the ability to communicate with customers or external third parties secure in the knowledge that all conversations and data are protected.
- **Data Privacy Compliant Communications** - Enable your organisation to remain compliant with your regulatory obligations and avoid fines. Keep total control of your data to meet GDPR [Data Protection Act] regulations, ensure data sovereignty and manage your information risk.
- **Operational & Cyber Resilience** - Create an 'out of band' communications capability that provides the ability to converse securely, even when standard IT systems are unavailable or have been compromised.
- **Compliant Collaboration** - Capture, archive and audit data across your communication channels whether just within your organisation, or with trusted partners, so you can respond to any internal or external audit or investigation, even if the conversations have been deleted from the original device.
- **Leverage BYOD** - Carry just one phone: turn your employees' personal mobile, desktop, tablet or laptop into a compliant device that securely separates business and personal communications and still have complete control over your data.
- **Cyber Threats & Data Privacy** - Ensure data and information is protected from eavesdropping, industrial espionage, attacks by nation states and other bad actors. Instantly revoke access for lost or stolen devices and wipe your secure data remotely.
- **Reduce Cyber Risk** - Mitigate the financial and non-financial risks posed by the use of unsanctioned and insecure consumer apps (often referred to as shadow IT).

Secure Communications Platform



Secure communications are a means by which people can share information with a high degree of certainty that the communications remain completely private. Third parties cannot intercept or overhear what was said, and the information shared remains in the control of the organisation from which it was sent (for example, information cannot be forwarded to other unauthorised parties).

Specifically, an enterprise secure communications platform like Armour Mobile™ provides many additional advantages over consumer grade apps, for example:

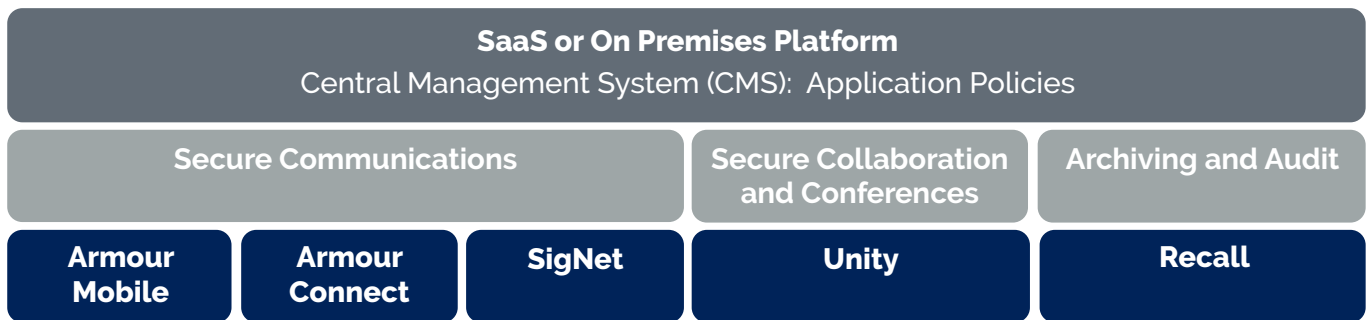
Centrally Manage Application Policies – define user settings centrally to ensure the appropriate security protocols are observed. Users can only be enrolled by an authorised admin, protecting all other users within the group or community.

Secure by Design & Secure by Default – Armour Comms has worked closely with the UK National Cyber Security Centre (NCSC) to ensure that all products are developed with Secure by Design and Secure by Default principles at their heart.

SaaS/On Premises Options – Armour Comms solutions are available with multiple deployment options. These include; as a hosted solution on Armour's secure cloud, as a Public cloud installation or as an On Premises implementation that provides data privacy as well as absolute control of your data and its sovereignty.

Secure Communications and Collaboration Solutions

Armour provides a secure communications platform, designed for use cases and scenarios where data is at higher risk



Armour Mobile™

Armour Mobile is Government and NATO approved for handling sensitive data. Enterprises will also benefit from the security features added as part of these approvals.

- Voice calls, messaging, video, conferencing and file attachments
- Identity-based authentication – be sure who you are communicating with
- Central Management System - add or delete users, control user data, manage security settings, remove wipe data if device is compromised
- Message Burn, automatically deletes messages on recipient's phone once read
- Management of data on BYOD devices including strong encryption of data at rest
- Add-ons include Enterprise Conferencing, Audit and Archive

Secure Communications and Collaboration Solutions


- Armour Connect™** Armour Connect provides interoperability options extending the reach of mobile secure communications to the desk phone in the enterprise.
- Integration with SIP, PBX, and other UC installations
- SigNet by Armour®** Entry level enterprise WhatsApp replacement that is highly engaging for users while providing powerful data security.
- Voice calls, messaging, video and file attachments
 - Message Burn capabilities
 - Data Sovereignty with Central User Management
- Unity by Armour™** Enterprise secure conferencing and collaboration solution that is easy and intuitive to use.
- Strong authentication – be sure who is on the call (no 'Zoom or Teams-bombing')
 - Video, documents and chat all remain protected within the Armour ecosystem
 - Message Burn for chats and attachments
- Recall by Armour™** Archiving and Audit solution providing the ability to record and playback messages, audio or video calls subject to strict security processes - essential for regulated industries.
- All transmitted media (text, attachments, audio) are archived
 - Tightly managed authorisation for audit access
 - Individual encryption keys limits access
 - All access to audit files is recorded

How people are using Armour

Armour Comms solutions support a wide range of use cases applicable across all security conscious markets

Here are some examples of critical use case scenarios where secure communication capabilities could be required.

Which of these use cases or scenarios might affect your organisation?

 <p>BYOD & Remote Working</p>	 <p>BCM & Disaster Recovery</p>	 <p>Mission Critical & Crisis Comms</p>	 <p>Manage Security Incidents</p>	 <p>Out of Band Comms for Cyber & Operational Resilience</p>	 <p>Comply with Regulations & Standards</p>	 <p>Secure Collaboration with 3rd Parties, Consortiums & Supply Chain</p>
 <p>Asset & IP Protection</p>	 <p>Vulnerable Communities & HR Related Scenarios</p>	 <p>C-Suite Protection</p>	 <p>Foreign Carrier & Networks Risk</p>	 <p>High Net Worth Individuals</p>	 <p>Combat Shadow IT</p>	 <p>Closed Messaging Applications up to SECRET</p>

How people are using Armour Mobile

Government



- SENSITIVE and SECRET within and across departments
- Extend secure collaboration out to trusted external partners
- Secure BYOD and remote working
- Out of Band communications – operational cyber resilience

Defence & Military



- Mission critical and sensitive data use case scenarios
- Secure communications up to SECRET
- Foreign carrier and network risk
- Use over satellite if required
- No requirement to use actual phone numbers
- Seriously robust security for organisations working collaboratively on bids, projects and research
- Secure collaboration with friendly forces, local contacts, and for training
- Audit facilities for all communications and associated files
- Central management of applications and security settings
- Data Sovereignty – control your own data at all times
- BYOD – Separate personal and business data
- Out of Band communications during a crisis

Critical National Infrastructure: Telco, Transport, Water and Energy



- Mission critical communications
- Out of Band communications – operational cyber resilience
- Secure collaboration with trusted external partners

How people are using Armour Mobile

Law Enforcement, Blue Lights & Justice



- Mission critical communications – alternative to Push to Talk
- Out of Band communications – operational cyber resilience
- Protect sensitive information within and across departments
- Extend security to vulnerable communities and informants
- Multiple agencies that need to collaborate using a secure communications platform
- Audit facilities for all communications and associated files
- Central management of applications and security settings
- Data Sovereignty – control your own data at all times
- BYOD – Separate personal and business data
- Out of Band communications during a crisis
- Securely issue documents like court orders to the front line
- Get control of your device and data - prevent recording and illegal retention of messages and phone conversations

Financial Services, Legal & regulated industries



- IP protection
- FCA regulatory obligations, compliance with regulations and standards
- C-suite protection
- Crisis communications for cyber and operational resilience
- High net worth individuals
- Supplier communications and risk management
- BYOD – Separate personal and business data

Enterprise



- IP protection
- Compliance with regulations and standards
- C-suite protection
- Out of Band communications – operational cyber resilience

Industry Accolades and Certifications

Industry awards including:



- **Queens Award for Enterprise.** 2021
- **SC Awards** for Best Mobile Security and Best Communications solution for Armour Mobile, SigNet and Unity by Armour. 2022, 2021, 2019



- **techUK & Tussell Tech200** – Top 20 Fastest-growing technology company in the UK public sector. 2022

Industry analyst review:

- Big 4 Analyst - **Leader** in Secure Communications quadrant

Security Certifications:

- ISO27001 certification
- Cyber Essentials Plus



National Cyber Security Centre



Armour's product offerings include Government and NATO approved solutions

Follow us:



www.linkedin.com/company/armour-communications-ltd/

www.armourcomms.com



Armour Communications Ltd

1st Floor, Millbank Tower
London
UK

SW1P 4QP

Tel: +44 (0)20 36 37 38 01

Email: sales@armourcomms.com