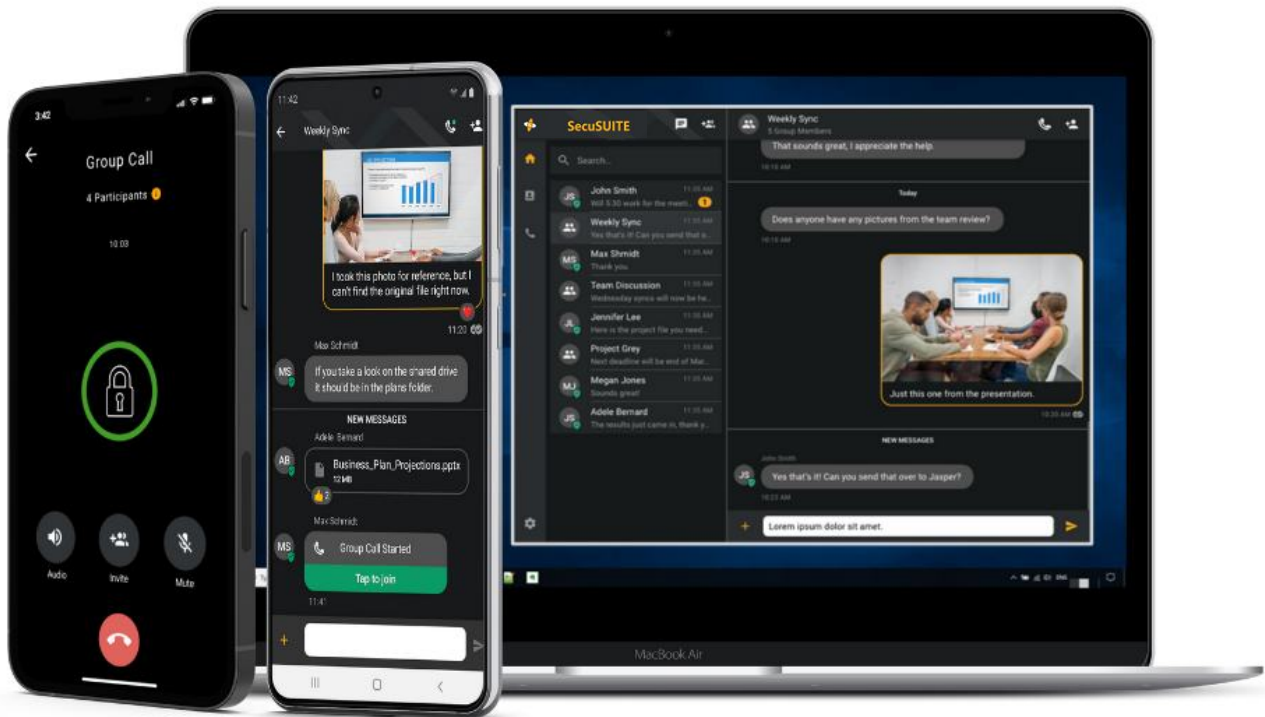# SecuSUITE®

High Security Voice and Messaging for iOS and Android

Current and Immediate Threats to Mobile Conversations

Imagine sophisticated cybercriminals and hostile state actors targeting your mobile phone to steal critical information. It's a harsh reality. Public networks offer them easy access to sensitive information, and traditional defenses crumble against ever-evolving mobile attacks. Today's threats are elusive and difficult to detect. Conducting serious business on mobile demands a serious solution – one that safeguards your vital communications and empowers secure collaboration.

Growing Geopolitical Tensions Are Causing:

- **Spike in mobile espionage:** State funded cyber intelligence operations employ highly sophisticated and difficult to detect mobile attacks for gathering high value data.

- **Increased economic warfare:** State sponsored eavesdropping on foreign commercial interests are now a widespread problem, costing billions in losses.

- **Active domestic threats:** Criminal enterprises, terrorist organisations, and rogue political entities actively engage in eavesdropping, conducting illicit operations, and settling scores against adversaries.

Surge Of Cyberattacks Threatens Mobile Communications

World governments and businesses rely heavily on smartphones to stay productive and connected. With this convenience comes increased risk. As sophisticated cybercriminals target mobile communications, it's crucial to safeguard your vital business information. Don't let your reliance on mobility become a vulnerability. Secure your communications and empower your team to collaborate safely, anywhere, anytime.

Many well known messaging apps leave you completely vulnerable. **500 million leaked WhatsApp accounts were compromised in 2022.**[1] Lack of transparency, administrative control, and certifications expose your conversations to attackers.

Your mobile **metadata** is far more revealing than your conversations. **More than two and a half billion personal records were compromised by data breaches in the past two years.**[2] Attackers are known to exploit your metadata which can expose your location and conversation history.

Many attackers today use clandestine methods to deploy malicious code to a user's mobile device to gain remote access to communication data. **67.87% of mobile attacks in 2022 were malware attacks.**[3]

[1] WhatsApp data leaked: 500 million user records for sale online | Cybernews
[2] Report: 2.6B records compromised by data breaches, underscoring need for E2EE - Apple
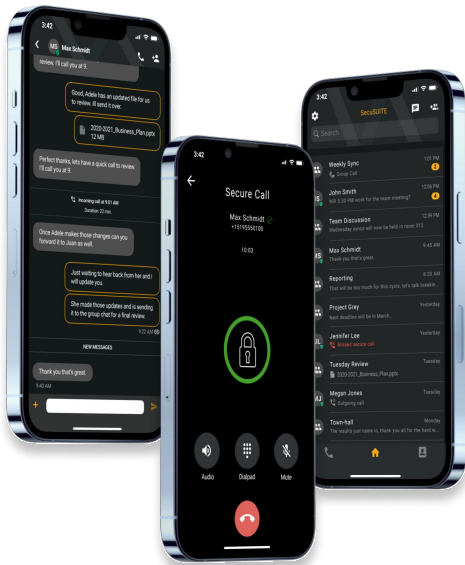[3] Mobile cyberthreat report for 2022 | Securelist

Ditch the Legacy Drag: Upgrade Your Secure Communication

Keeping valuable information secure is critical, but legacy solutions are falling short. While traditional mobile voice apps and landline encryption offer some protection, they either limit mobility, flexibility, or security, hindering real-time secure communication in today's fast-paced world. You need secure communication that empowers you to collaborate seamlessly from anywhere, on the go, without compromising on security.

SecuSUITE® - Serious Solution For Serious Business

Secure your mobile conversations anywhere, anytime with SecuSUITE. Our cross-platform solution safeguards your business communications on both Android and iOS devices. SecuSUITE goes beyond basic app encryption, offering the highest level of security to protect against even the most sophisticated mobile attacks.

Boost your Business Productivity with Confidence

Designed to Protect High Value Communications

SecuSUITE delivers military-grade security design and is backed by rigorous independent third-party Common Criteria validation and certification - achieving approvals for communication up to Top Secret.

Verified Community of Contacts

Every user is always authenticated so you can be sure of who you're communicating with. No spooking, deepfakes, or social engineering on your network. SecuSUITE gives you the peace of mind of proven security.

Maintain Ownership of Your Data

Don't put your trust in consumer-grade cloud platforms, take sovereign control of your data and comply when needed with regulatory requirements for archiving and auditing.

Strengthen your Organisation's mobile security posture with:

- End-to-end encrypted voice and messaging with admin management of group conversations.

- Group calls with up to 20 people and access to an authenticated contact list, including VIP privileges.

- Organise, join, and manage large conference calls by integrating with your organisation's PBX system.

- Admin console for account management and full system control.

- Integrate your devices with certified Mobile Device Management platforms.

- Administer your user community into multiple tenants, so users can be organised into functional or project groups to safeguard 'Need to Know' principle.

- Protection against metadata collection by external parties and meet all regulatory compliance requirements.

- Deploy on-premises for full data sovereignty, cloud, or as a field-based tactical system.

SecuSUITE's Record Of Credibility

NIAP Approval and Common Criteria Certification
Common Criteria Certified and listed on NIAP Compliant Product list and U.S
Commercial Solutions for Classified (CSfC) component list

FIPS 140-2
Use of FIPS 140-2
approved crypto
modules

**NIST - National Institute of
Standards and Technology**
Achieved certificates for all
cryptographic materials used in
product - Cryptographic Algorithm
Validation Program (CAVP)

NATO Approval
Security Accredited and
Approved for NATO
RESTRICTED

**Canada Secure
Tailored Solution
(STS)**
Approved for
Government Canada
Secret

Contact Us To Secure Your Communications

VISIT WEBSITE

WATCH VIDEO

REQUEST DEMO

BlackBerry® | secusmart

For more information, visit BlackBerry.com and follow @BlackBerry.