Retain Secure Mobile Messaging Compliance Solution

The Retain™ Secure Mobile Messaging and Compliance Solution* delivers secure, encrypted messaging for iOS and Android devices to organizations around the world. This solution is for organizations that use personal employee and corporate devices to generate and consume business data, while helping them meet regulatory and compliance requirements. Retain is the only enterprise-acceptable solution to provide iOS and Android device data archiving without the need to tether the device or sync the data.

Key Features

Retain Secure Mobile Messaging and Compliance Solution Includes:

- CellTrust SecureLine
- Retain SecureLine Collector
- Retain Unified Archiving

CellTrust SecureLine provides your organization with encrypted communication for iOS and Android devices. Its dedicated SMS, or text, message gateway has an encrypted SMS message connection, uses an iOS or Android app to separate business data from personal data, and includes an encrypted phone line with a dedicated business phone number.

The SecureLine Server logs and routes all subscriber and non-subscriber communication. All encrypted messages are received by the server and are routed directly to the intended recipient. Electronic communication, including text messages, voice calls, secure messages, and separate business number call data, is decrypted and logged by the server. The server offers multiple layers of authentication and can be deployed on-premises or in the cloud.

The CellTrust SecureLine Mobile Device App is a password protected app that can be installed on any corporate or personal iOS or Android device. The app separates the device's storage into two separate partitions: one for business and the other for the employee's personal data. It has secure-server registration, multi-factor authentication, 256-bit AES encryption with unique dynamic keys, and full encryption key lifecycle management. The app can be downloaded from The App Store or Google Play.

This Solution Includes:

- A separate encrypted phone line with its own dedicated business phone number
- An encrypted SMS message connection
- iOS and Android apps that separate business data from personal data
- iOS and Android apps that only store business related data
- A complete archive of all business communication, which includes search, publishing, and eDiscovery tool capabilities

_____

*Not available in all countries

Secure Mobile Messaging for Android and iOS

Retain Unified Archiving is the only enterprise solution to provide iOS and Android device data archiving without the need to tether the device or sync the data.

This Solution Includes:

- A separate encrypted phone line with its own dedicated business phone number
- An encrypted SMS or text message connection
- iOS and Android apps that separate business data from personal data
- iOS and Android apps that only store business-related data
- A complete archive of all business communication, that includes search, publishing, and eDiscovery tool capabilities

Encrypted Phone Line:
Employee phone conversations are secure and are encrypted, which eliminates the concern that private phone calls are being intercepted and monitored or that organizational data could be leaking out of your organization without your knowledge.

Dedicated Business Phone Number:
Enables users to have a business phone line that is separate from their personal phone line. Each employee receives a new dedicated virtual business number, which also allows them to use their existing SIM card. The app creates a separate log, record, and audit trail of all business SMS/Text and voice communication. Employees no longer need to provide their personal cell phone number for use in business purposes.

Encrypted SMS/Text Message Connection:
All employee SMS/Text message conversations are secured and encrypted. This alleviates the concern that your SMS/Text messages are being intercepted or monitored, and it provides a high level of security to prevent mission-critical information from getting into the wrong hands.

iOS and Android Apps Separate Business Data from Personal Data:
When business data is generated and consumed, it is kept entirely separate from personal files. Whether the mobile device app is running on an iOS or Android device, your employee's photos, contacts, SMS messages, emails, GPS location, and financial data are kept separate from any SecureLine electronic business communication.

Internal Messaging: All internal business SMS messages are encrypted by the SecureLine app and are delivered to the intended internal recipient via the CellTrust SecureLine Server.

External Messaging: All external business SMS messages are encrypted by the SecureLine app and delivered to the intended external recipient via the SecureLine Server. The SecureLine Server passes the message to the carrier, and then it is delivered to the standard SMS inbox of the non-subscriber, regardless of the type of device. When the non-subscriber responds to the message, it is sent to the carrier, and the carrier sends the message to the SecureLine Server. The server logs the message and delivers it to the subscriber's device.

Complete Archiving of all Electronic Communication with Case Assessment, Search, and eDiscovery:
Retain Unified Archive communicates directly with the CellTrust SecureLine Server, and pulls down all encrypted SMS messages and phone logs through an encrypted connection. The Retain Collector then routes that data directly to the Retain Unified Archive. It collects all SMS messages and phone logs and archives all conversations in context. Retain provides multi-platform unified message archiving of all email, social media, and mobile communication data for case assessment, search, and eDiscovery and can be deployed on-premises or in the cloud.

MICRO FOCUS®