TreeBox
Solutions
Secure Mobile Communications

OnTalk®

Whitepaper: 10 Questions to ask when choosing Secure Communications Solution.

OnTalk® is an award-winning solution that secures your voice calls, conference calls, instant messaging, group messaging, attachments and in-app media capturing. OnTalk® defends you against data leakage, privacy violations and keep your communications private.

Military-Grade Encryption . Award-Winning Solution. Unrivalled Simplicity

1 Commonwealth Lane #03-01 Singapore 149544   Tel: 6570 3725   website:www.treeboxsolutions.com

10 Questions You Need to Ask

Question 1 – Does the solution protect your contact list and information?

Many of the free and unsecure messaging solutions rely on the phonebook for contact information. However, the phonebook can be compromised without the user’s knowledge. There is no guarantee that the phonebook entries cannot be faked once the free and unsecure messaging apps extract these information from the user’s mobile device.

A good and secure messaging solution will protect your Enterprise’s contact list. The Enterprise’s contact list must be authenticated and provides you with the assurance that your callee is really who he or she is.

Question 2 – Does the solution authenticate the callees?

How do you know that your callee is indeed the person that you are calling? Can the contact list be spoofed?

A good and secure messaging solution will ensure that only authenticated users are connected into the solution. It will ensure that when you want to make a secure call, the callee is authenticated and cannot be spoofed.

Question 3 – Does the solution encrypt the voice calls, messaging and SMS?

Many of the free apps are unsecure. They do not provide any encryption to protect the conversations. It is important for Enterprises to look for solutions that provide encryption for data-at-transit and data-at-rest. Data-at-transit refers to communications information that is moving from one device to another device while data-at-rest refers to the protection of the information on the mobile devices.

Question 4 – If the solution provides encryption, does it use a different encryption key each time?

Some of the solutions that provide encryption uses a pre-shared key concept. This means that all conversations are encrypted by a single key and this single key is also shared with all other users. Obviously this design does not provide any protection at all since a single key can be compromised and put all other users’ secure conversations at risks.

A good and secure communications solution would generate a new encryption key for every new call.

Question 5 – Does the solution prevent the media information to be leaked out?

Today, many solutions do not take care of the media content – i.e. the pictures, audio files and video files. These media content in the mobile devices represent the assets that are at risk. Most solutions do not protect these media files.

A good and secure communications solution would ensure that such media files cannot be leaked out or send to any unauthorized recipient.

Question 6 – Does the solution provide centralized management and control?

Many of the free and unsecure messaging solutions rely on the principle of “self-management”. Individual users download the apps and start to communicate with each other. However, from an Enterprise’s perspective, it is important to be able to centrally manage and control the solution. This allows Enterprises to dynamically add, delete, amend users as well as control the secure services that can be granted to the users. This also allows Enterprises to remove ex-employees who have left the company, and ensure no sensitive data resides in the ex-employee’s mobile device.

Question 7 – Does the solution give the Enterprises full assurance?

Enterprises need to get assurance that the solution is secure and there are no possibility of backdoors or trojans. Often the free messaging apps are deployed in public cloud where there is little control on the access and exposure of the content to unauthorized person. A good solution will provide an On-Premise deployment that can meet the Enterprises’ assurance level and security policies.

Question 8 – Does the solution provide audit logs?

Many of the free messaging apps do not provide a system to track access and risks. Often, such apps are deployed in public cloud where the accessibility and control are not known. This puts the Enterprises at risks. A good solution will provide full audit logs that can allow Enterprises to trace and monitor risk exposures.

Question 9 – Is the solution designed by experts?

Many products claim to offer encryption but not many developers know how to use the encryption technology properly. For example, a solution can have the best lock (encryption algorithm) and the strongest key (key to unlock), if the key is not properly handled, such as leaving inside the lock after usage, this would compromise the security.

A good solution needs to be designed by security experts where security is designed from Day 1 and not an after thought.

Question 10 – Is the solution being evaluated or validated by other experts?

A good solution should be validated independently by a third party or by the customers. This ensures that the design of the solution is implemented as claimed.

In TreeBox, we have designed a solution – OnTalk® that can effectively address all these 10 questions. Our solution is secure, designed by security experts with independent verifications and provide full suite of security services to protect the voice calls, messaging, SMSes, attachments and media. We ensure that the mobile content that is generated with our app is well protected and users have full assurance of a secure solution.

OnTalk®, Protects your privacy

TreeBox Solutions

OnTalk® – Your Privacy is our Priority.

OnTalk® is an award-winning solution that is designed to protect the Enterprise sensitive conversations on mobile devices. OnTalk® secures voice calls, conference calls, instant messaging, attachments and SMS. Embedded with the strongest encryption algorithms and security protocols, OnTalk® aims to deliver the highest assurance to Enterprises. Not only OnTalk® is extremely easy to use and deploy, OnTalk® also provides options for Enterprises to own and have full centralized control of users. Enterprises can dynamically create, amend, delete users and manage the secure services that are granted to each user. This solution gives control back to the Enterprises.

Why Customers Choose OnTalk® ?

- **Secure & Trusted Solution - Developed by Security Professionals**: OnTalk® is developed by a team of experience security professionals. Backed with many years of relevant experience, TreeBox understands the security requirements and ensures that optimal performance is delivered to customers in a robust, reliable and resilient manner.
- **One-Touch Design Concept - Extremely Useable**: At TreeBox, we believe that any security solution must be designed with the user in mind. A secure but inconvenient solution will not be useful. Instead, TreeBox adopts a design principle - "One-Touch Concept" where all basic functionalities can be accessed via One-Touch from the user. TreeBox has impressed customers with the extremely useable solutions.
- **Innovation - TreeBox developed OnTalk®**. The entire solution is developed in-house and TreeBox has filed two international patents for its innovation.

About TreeBox Solutions – Raising the benchmark in mobile security

A pioneer in military-grade secure communications solutions, TreeBox has grown to become a leading mobile secure communications provider across Asia Pacific. With deployments in more than 14 countries and with offices in Singapore, Japan and USA, TreeBox provides best secure solutions for customers.

Contact Us: Sales@treeboxsolutions.com

OnTalk® – Market Leading Mobile Security Features & Capabilities

Secure Real-Time Contact List

Enterprises can control and configure a separate business contact list.

Secure Voice Communications

End-to-End encryption with crystal clear voice quality calls. Secure Conference calls supported.

Secure Instant Messaging & SMS

Secure 1-to-1 and group IM.
Secure SMS does not require data connection.

Secure Attachments & Media Mgt

Attachments are securely stored within app. Manage sensitive files privately.

Secure In-App media capturing

Capture and share photos or videos directly from app without appearing in photo gallery.

Secure Broadcasting

Broadcast securely to entire team with instant acknowledgement.

Military Grade Encryption & Security Protocols

Highly classified information is secured via OnTalk® Security Card