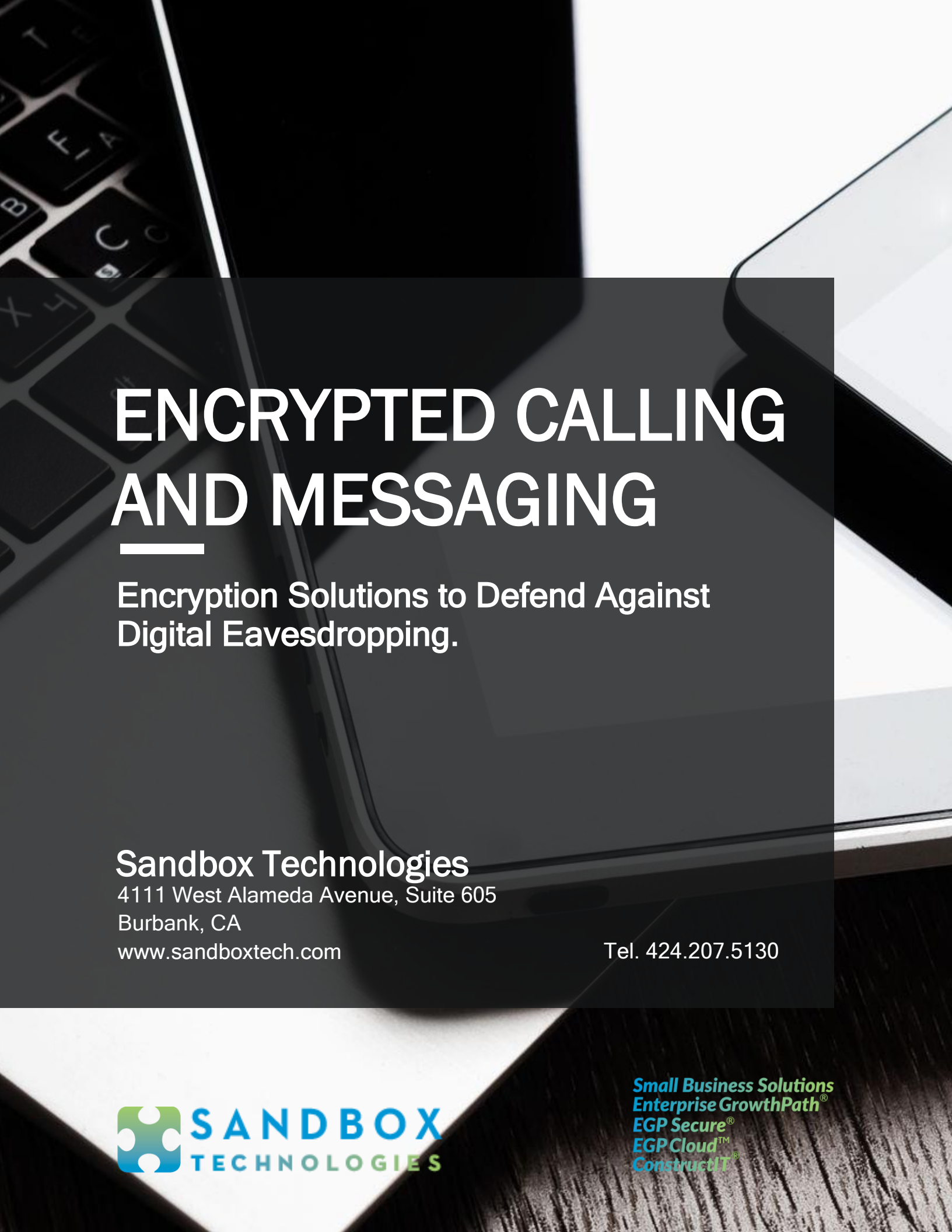

ENCRYPTED CALLING AND MESSAGING

Encryption Solutions to Defend Against Digital Eavesdropping.

Sandbox Technologies
4111 West Alameda Avenue, Suite 605
Burbank, CA
www.sandboxtech.com
Tel. 424.207.5130

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Encrypted Calling and Messaging

Defend against digital eavesdropping with end-to-end encryption.

When it comes to business communications, two important trends are converging. First, an increasing number of work conversations take place on mobile devices via voice and text. Second, electronic privacy is becoming increasingly vulnerable to being compromised. If confidentiality is important to your business, protection against digital eavesdropping is vital.

Are You Meeting Privacy Expectations?

Business users can be cavalier about privacy when making voice calls and texting. Some assume that their mobile connections aren't vulnerable; for others, privacy issues just aren't on their radar, perhaps because they don't work in industries where privacy is a focus or mandated by regulation.

Communications don't need to fall under the umbrella of attorney/client privilege or physician/patient confidentiality to require privacy - although these categories certainly come to mind. The reality is that most business communication comes with an expectation of privacy within the organization; for example, contract negotiations, employee recruitment, financial consultations, sales efforts, and the like can be highly detrimental if read or heard by persons not a party to the conversation.

The truth is that mobile voice calls and texts are vulnerable to eavesdropping at serval points from end to end. Encrypted calling and messaging helps protect private exchanges of information with employees, clients and coworkers.

Shield Mobile Communications

Many organizations mistakenly believe that most modern mobile communications are encrypted but that's very often not the case. In fact, many solutions are not only vulnerable, but depending on the messaging app being used and the device the user is texting to, some are actually being exploited by the very providers of the communication platform.

Although standard SMS text messages are sometimes encrypted by the service provider, the encryption used to protect text messages is known for having numerous weaknesses, in addition to the fact that service provider often has access to the message content.

End-to-end encryption helps to protect electronic communications, whether it's via voice call, text, group chat or attachment. By encrypting messages at both ends of a conversation, only the sender and the receiver of the messages have the "keys" to read them. Entities intercepting the messages in transit – know as "man-in-the-middle attack" – receive only encrypted data, preventing everyone but the most sophisticated eavesdropper from deciphering them.

For additional information, contact your Sandbox Technologies Engineer, Account Manager or Consulting CIO, or send an email to inquiries@sandboxtech.com.