appdome

Appdome for Legal Services

Ensuring trusted mobile services for lawyers and law firms

Today's legal industry is fast becoming mobile at every level. Mobile promises unique opportunities for law firms as they strive for more efficient practices and better service delivery models. Lawyers and staff are demanding more mobile solutions to collaborate, communicate, work and serve their clients' needs via their mobile phones and tablets. Appdome helps law firms secure mobile apps that serve lawyers, legal professionals and clients alike.

THE ROLE OF MOBILE APPS IN LEGAL

Mobile apps have a big role in the legal industry. General-purpose mobile apps used for human resources, training, internal collaboration, expenses, VoIP communication, and other common enterprise services – like Jabber, WebEx and ServiceNow – have found their way into law firms.

In addition, special-purpose mobile apps designed for the legal industry – such as iManage, BigHand and Aderant – have emerged to allow professionals to perform everything from timekeeping, to dictation, document production, document sharing, client communication and resourcing.

Some law firms have begun internal development of mobile apps. Others are using specific mobile apps with specific clients, sharing environments to deliver the best service to clients.

MOBILE SECURITY IN LAW FIRMS

Law firms occupy a position of trust with their clients. The services they perform are inherently confidential at every level. The use of mobile apps in the legal industry presents a unique mobile security challenge.

The rules of professional conduct require lawyers to keep client communications, information and documents confidential, and communicating or storing data by means that are insecure or vulnerable to hacking may give rise to an ethical violation and jeopardize the attorney-client privilege.

When law firms use mobile apps to perform legal work, they must address the security of the app across multiple interdependent dimensions, including the app's user, data, services and access. This is true whether the app is built internally or licensed from third-party app vendors.

It is this unique challenge that holds back the adoption of mobile apps at many law firms – justifiably, in light of recent security breaches at law firms that have undermined trust and confidence in their services.
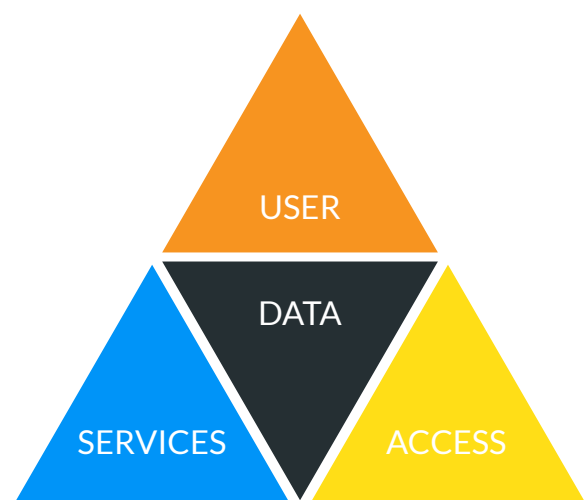

Figure 1: The security model for mobile apps in the legal industry is mutli-faceted.

TOP 3 SECURITY CONSIDERATIONS FOR LAW FIRMS

Appdome recommends a three-pronged approach to securing mobile use at law firms.

Protect Mobile Apps

Sound security policy begins by protecting the app itself. Whether the law firm builds the app itself or licenses the app from a third-party app vendor, the code and resources used by the app should be protected by advanced security methods and technologies. Law firms shouldn't assume that app makers build their apps with the security needed by the legal profession.

Solution: ONEShield™ by Appdome provides security for apps. This service includes code obfuscation, encryption for strings and in-app preferences as well as anti-tampering and anti-debugging and other app hardening mechanisms, all of which stop hackers from getting access to sensitive resources, user credentials, user names, as well as discovering the structure of the app itself.

Protect Mobile Data

All apps, or better said, all app users generate data on mobile apps. When used by lawyers, that data is confidential and needs to be protected, certainly when the data is client data. Mobile data is stored either in the application sandbox or in memory. Without encryption for this data, hackers (even casual hackers) can access client and/or privileged data and learn confidential information about firm clients.

Solution: Appdome Security Suite and Appdome for EMM each provides law firms multiple options to encrypt app data. Commonly known as data-at-rest encryption, or DAR, these methods secure app data wherever the data resides. The Appdome Security Suite and Appdome for EMM also provide different solutions to protect and encrypt the data while in transit.

Protect Mobile Access

Users access apps and apps access services and networks. Protecting how users access apps and how an app accesses these services and resources is of paramount importance. To ensure authorized use of apps, law firms can enforce app-level PIN codes, touch-ID or advanced authentication services from EMM, MDM or identity providers. To ensure that apps access only approved resources, law firms must consider advanced techniques like supporting dedicated or EMM-specific VPNs, direct connections to secure browsers and secure email systems, private certificates, and similar strategies. Similarly, the connection between the app and the server (hosted in a public or private cloud) needs to be encrypted to prevent any data leaks during transit.

Solution: Appdome for EMM with Appdome Mobility Suite and BoostEMM™ from Appdome provides law firms the ability to add EMM and MDM systems and support multiple use cases including user authentication, VPN, Single Sign-On (SSO), and direct connections to secure browsers and secure email systems. Appdome Mobility Suite also fully supports private certificates, layered proxy support and other strategies to protect mobile app access to law firm environments.

To learn more about Appdome for Legal Services, visit **www.appdome.com** or open a free Appdome account and start fusing!