zscaler®
Secure. Everywhere.

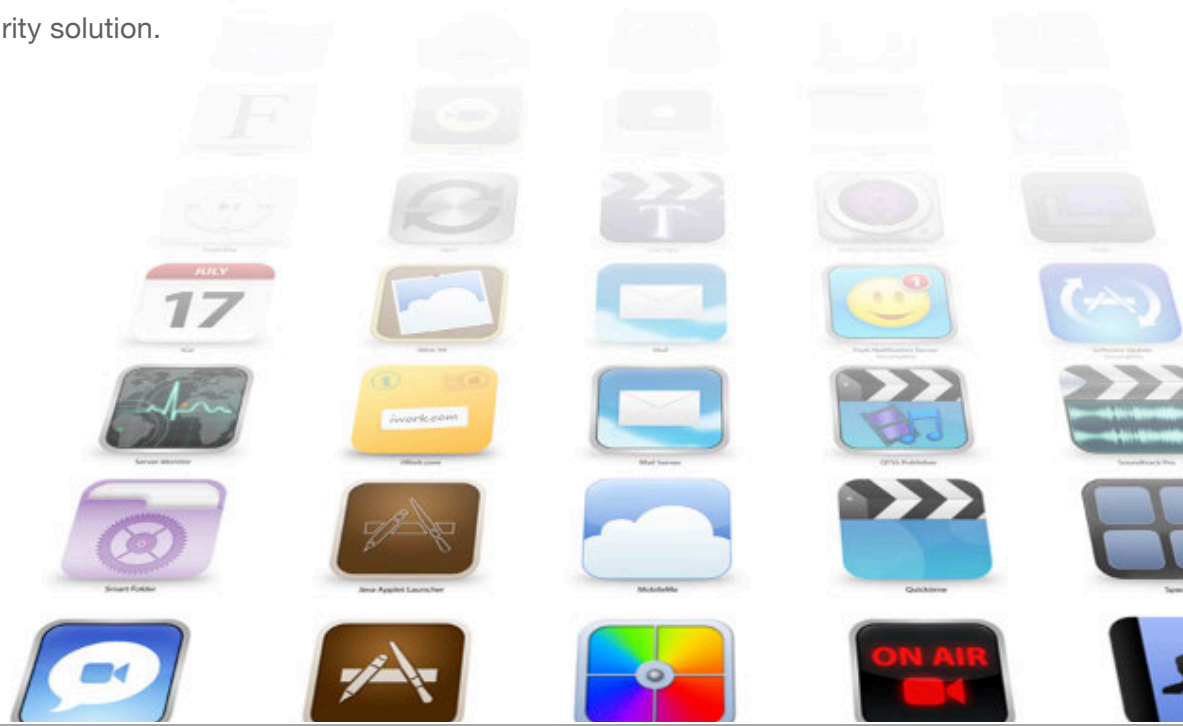
4 Steps to Effective Mobile Application Security

Table of Contents

Executive Summary

Mobile devices, and the advantages they offer, have changed the way we do business and even live. However, smartphones and tablets have also have wrought a new class of security threats and attack vectors. The varied mobile platforms and devices, along with the exponential growth of mobile apps can quickly become a security and compliance nightmare for enterprises to manage. While no one seriously thinks we can turn back the clock on mobile device and mobile app usage, new and more effective security measures are required. Security industry offerings that tried to graft existing PC era security technology onto mobile devices as well as mobile device management (MDM) solutions have proven inadequate to properly secure mobile devices and the networks they are accessing

True mobile security requires the ability to understand and classify mobile applications through traffic patterns, identify threats in real time and enable quick corrective action. This white paper discusses the - challenges surrounding mobile application security, the shortcomings of traditional solutions and details the 4 necessary attributes for a robust mobile security solution.



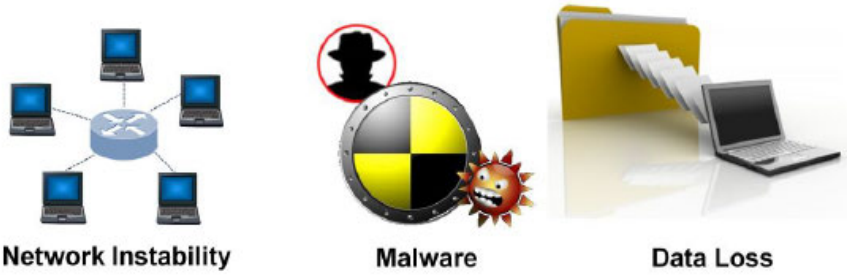
Mobile Security Risks in Enterprise Environments

Smartphones and tablets have rewoven the very fabric of how we work, communicate and even live. This revolution has occurred due to the ability of these devices to access and utilize both personal and corporate applications. There is literally an app for everything. Combine this with the Moore's Law-like exponential growth in computing power in mobile devices and near ubiquitous connectivity, one can easily see why mobile devices are increasingly viable replacements for traditional devices like laptops and desktops.

Epitomized by the BYOD trend, mobility offers the benefits of greater communication and efficiency for workers and the organization. This has led to as many as 95% of organizations adopting BYOD in one form or another. But a greater depth of BYOD adoption is meeting resistance from IT and security teams as they worry about the security implications of BYOD.

A recent Gartner report calls out network instability, risks of malware and risks of data loss as key impediments to greater BYOD adoption. BYOD and mobile devices have given rise to a new vector for security threats, rendering traditional security approaches ineffective. New approaches to security are necessary to address the threats that mobile devices – both company issued and BYOD - pose.

Three Risks of BYOD



SOURCE: *Gartner*

The Shortcomings of Traditional Security Approaches

Traditional appliance-based security was designed to protect internally based corporate-owned computers and corporate applications run inside the perimeter. Mobile devices by their very definition are not constrained inside the corporate network. For that matter neither are corporate applications, with many enterprises adopting cloud-based business applications. Employees, partners and customers are increasingly mobile and remote. With both devices and applications now extending outside the corporate network, it is little wonder that traditional appliances designed to protect inside the network are ineffective in protecting contemporary devices and applications.

A second driver for new mobile security solutions is the capabilities inherent in the most popular mobile apps. Research by mobile security teams indicates that more than 60% of the top 50 popular iOS and Android apps were either Games or Entertainment apps. Apparently, 70% of the top 50 Apple iOS apps have access to device location, 52% read user contacts, and 88% of them communicated to external advertising websites[1]. The risks of personal apps reading sensitive information off the device

[1] *Mobile App for Kids: Disclosures Still Not Making the Grade — FTC Staff Report December 2012*

and transmitting it to remote potentially unknown servers are inherent in the overwhelming majority of mobile applications.

Finally, the Android platform in particular has gained negative publicity recently. Perhaps a victim of its own success, Android has been targeted by criminals. Malicious Android apps, typically hosted in unauthorized app markets or on malicious websites, have been the culprit in several high profile incidents. Unsuspecting users are lured to such markets or websites via false ads or phishing scams.

Android is however not the only mobile OS with security issues. Even Apple's vaunted "walled garden" approach has exhibited security issues. Another factor for both Apple and other mobile devices is the large number rooted or jailbroken devices. Such devices allow potentially malicious apps to be installed bypassing Google and Apple's own security screening.

Initial Security Industry Solutions for Mobile Security

The Security Industry, confronted with the reality of mobile devices and the BYOD movement, responded with two primary types of solutions:

1. **Anti-malware suites**: Similar to the anti-malware suites on traditional desktops and laptops, these solutions start with AV engines (both behavior and signature based) and add a "kitchen sink" of other security technologies. There are white lists and black lists (of web sites, applications and behaviors), DLP, IPS, Spam filter, etc. Again very similar to their desktop brethren, they try to package as many endpoint security technologies as possible into one suite. It is ironic that at a time when so many in the security industry are saying desktop AV and anti-malware are near useless, the same technology is being repackaged for mobile devices. If it is not working on the desktop, what makes us think it will work on mobile devices?

2. **Mobile Device Management (MDM)**: Originally touted as the killer app of BYOD, MDM allows enterprises to set and en force policies regarding mobile devices that are granted access to the network. MDM allows administrators to set and enforce configuration profiles and even provides the ability to lock, locate and wipe remote devices. MDM also provides some control over which allowing or blocking mobile apps using a white list/black list approach.

   IT and Security teams have come to the realization that MDM solutions while useful are not a panacea. Even with anti-malware integration, MDMs cannot address the risks of advanced threats like phishing and spyware. They are also unable to protect from malicious apps, as they are not capable of real time monitoring and cannot provide proactive defense.

The Key to Mobile Security is Mobile Application Security

Mobile devices such as smartphones and tablets need comprehensive mobile security solutions that extend beyond Mobile Device Management (MDM) and anti-malware suites. The key to effective mobile security is understanding, managing and enforcing policy regarding mobile applications.

A comprehensive solution must enable enterprises to not only protect mobile users from threats, malware and security compromises, but also proactively defend and monitor corporate resources while they are being accessed by mobile devices. This requires real-time real time visibility and the ability to enforce policy on mobile apps.

Real time Application Visibility

True app security starts with the ability to *identify* apps in real time and *categorize* them based on traffic patterns.

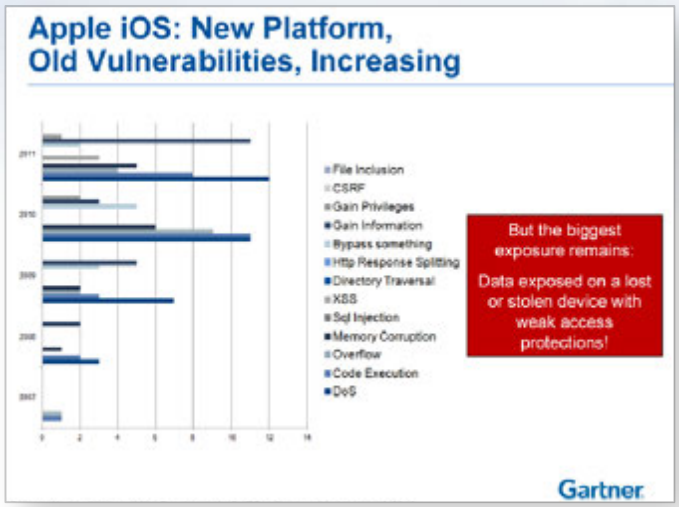
Identifying Applications

Identifying apps by their name and categorizing them by whether they are games, video, etc. is a necessary first step but is not sufficient. It is imperative to inspect the actual mobile app traffic and identify patterns - Where does the app send traffic to? What is the nature of that traffic? What is the propensity for that app to be malware or misbehave? To be effective in a mobile environment a security solution must be able to identify any suspicious traffic from the app, such as contacts, geo-location or user identity being sent to remote servers. Apps once identified can then be classified by the nature of traffic they generate.

Another aspect of application identification is to identify where the app came from. In addition to corporate apps distributed by the enterprise, users can download apps from main stream app markets (ie. iTunes, Google Play, Windows Store) or from 3rd party and unauthorized mobile markets. Unauthorized mobile markets are often found to host malicious apps. Users may be redirected or phished to an unauthorized mobile market without being aware of it. By stopping such redirection and preventing users from installing these apps and introducing them into the network, the level of security around mobile devices can be noticeably raised.

Categorizing Applications

Once applications have been correctly identified, they can be categorized based on standard market categories as well as their propensity to be malicious and/or leak confidential information. Categorizing applications allows for the setting and enforcing of policies to protect the enterprise network, confidential information and the mobile user.



It is important to note that to be effective, identifying and classifying apps require *continuous real time visibility* into application traffic. The nature of the threat is one that is ever changing. While an application may at first seem innocuous, circumstances or factors can change which could render it potentially malicious or harmful. Analyzing mobile app traffic on an ongoing basis allows for up-to-date intelligence into the character of mobile applications, and supports immediate remedial action when required.

Most security solutions only profile apps based on their market category and cannot analyze actual network traffic. Traditional web security or web filtering techniques such as those in some of the anti-malware suites only analyze traffic at the URL layer. This is ineffective in understanding mobile app traffic which may not use URLs at all. Traditional IPS and firewall products are equally ineffective at identifying malicious mobile apps malware because mobile traffic requires a higher-layer inspection than most contemporary IPS or firewall products offer.

Application Control

Once mobile apps on the network are correctly identified and classified, organizations must *set policy* and run *real time reporting* to ensure compliance.

Setting Application Policy

Corporate policies can be set to restrict traffic based on app category and/or the risk the app poses to the enterprise. This helps to better articulate compliance standards to employees, and enables administrators to take proactive steps to restrict mobile app based on the nature of traffic. For example, it may turn out that a popular video streaming app is causing high network usage and hence needs to be restricted during work hours, or that a popular gaming app is leaking location and device information to a remote server and is therefore a risk on the network. Enforcing restrictions on mobile apps transcends traditional URL filtering mechanisms, as mobile apps generate traffic to a variety of URLs and domains, unlike traditional browsers connecting to the same applications.

Real time enforcement

Once policy is set, enforcing compliance is the next logical step in the process.

Staying ahead of contingencies and threats requires that administrators are able to not only detect violations in real time, but also enforce remedies in real time. For example, if an employee connects to corporate resources from a device with active mobile malware on it, it is necessary to block all malicious traffic from the device and identify both the user and device associated with the incident.

This real time element and ability to block malicious traffic can be the most vital aspect of mobile application security. The fact is that even with an MDM solution in place, some users will become infected with active mobile malware. Waiting until the repercussions of the infection become obvious is not pragmatic. An effective security solution must be able identify the infected device and associated user in real time and enable immediate corrective action to protect the user and the corporate network.

Conclusion

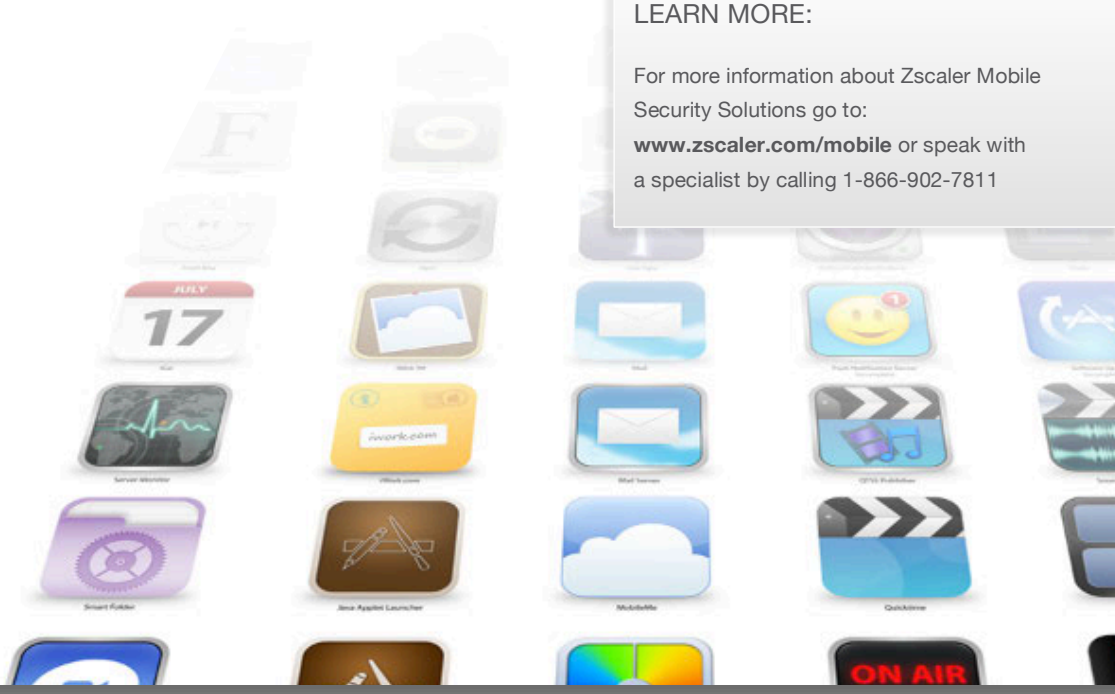
Today, an individual user's smartphone is often one of his most important devices, having email, stored passwords, personal data from social networking sites and even access to a host of business and financial services. There is no doubt that mobile devices have changed the way we work and live.

While mobility offers several advantages, mobile technology with its plethora of applications also presents new security challenges that traditional security solutions are ill-equipped to deal with. Taking anti-malware from desktops and moving them to phones and tablets is not enough. MDM solutions provide device management, but do not protect against advanced security and mobile application threats. While white listing/black listing of mobile apps attempts to give administrators control over mobile applications, the fast changing nature of the mobile application market renders it ineffective.

Mobile security demands purpose designed solutions that acknowledge the ubiquitousness of mobile applications and address the unique security challenges they pose. To be effective, the solution needs to provide in-depth visibility to and control over mobile applications. Consistent monitoring of mobile application traffic, identifying applications based upon traffic patterns, building and enforcing policies based upon this analysis, and having real time reporting and remediation are the building block to truly secure mobile application usage in enterprises environments.

LEARN MORE:

For more information about Zscaler Mobile Security Solutions go to: **www.zscaler.com/mobile** or speak with a specialist by calling 1-866-902-7811



About Zscaler

Zscaler is transforming enterprise security with the world's largest security cloud, built from the ground up to safely enable users doing business beyond the corporate network. Zscaler's security cloud processes over 8 billion transactions a day with near-zero latency to instantly secure over 10 million users in 180 countries, with no hardware or software required. More than 3,500 global enterprises are using Zscaler today to simplify their IT operations, consolidate point security products, and securely enable their business for mobility, cloud and social media. For more information, visit us at **www.zscaler.com**.

Copyright © 2013 Zscaler, Zscaler®, and the Zscaler Logo are trademarks of Zscaler, Inc. Mobile App Security Whitepaper