WHITE PAPER

Acronis®

Mobile Security

Top Five Security Threats for the Mobile Enterprise and How to Address Them

Today's countless mobile devices present tangible opportunities to drive measurable and substantial value for the enterprise. Field service workers, executives on the go, sales reps, project managers and others all have a need for mobile access to applications and enterprise files. It's no question that the advent of the iPad® and other mobile computing devices brings substantial benefits to the enterprise.

However, these benefits also come with new security risks that enterprise IT departments must be ever vigilant about, lest critical data be compromised. The consumerization of IT and BYOD (bring your own device) programs in the workplace make mobile file management (MFM) solutions more important than ever before.[1] In this white paper, we'll cover the latest security threats to the mobile enterprise, as well as solutions to overcome them. Solutions that allow enterprises to make the most of the benefits iPads and other mobile devices bring to the company while safeguarding security, and help to foster happy employees, increased productivity, and streamlined, managed workflows are increasingly critical in today's enterprise IT landscape.

Security threats include:

1. Unsecure File Transfer
2. Lost/Stolen Devices
3. Open Wi-Fi Networks and Public Hotspots
4. Malware and Viruses
5. Unclear Corporate Policies

Unsecure File Transfer

Problem:

iPads and other tablets make mobile file management a bigger issue than ever before due to the lack of native file storage on the devices. Employees typically opt for consumer-driven workarounds and synching solutions, which, according to recent filings with the FTC, do not live up to their guarantees of secure, encrypted file transfer and storage.[2]

Solution:

Mobile file management provides simple, secure and managed access to enterprise files on mobile devices. Without it, employees can retrieve and interact with corporate files on mobile devices that open your organization up to serious risks. Workarounds such as using consumer synching services to store corporate assets for mobile and offline access–leaving files unprotected and access unmanaged by IT–create opportunities for breached security and unmet compliance. Solutions that ensure file access is password-protected and encrypted in transit as well as on-device protect critical assets while enabling employees to work on the latest mobile devices. The optimal solutions integrate into existing corporate security environments, such as instantly with Active Directory and allow organizations to use existing data center infrastructure and servers, rather than third-party add-ons. These features allow corporate IT to remain in control and provide the greatest oversight for optimal security and compliance.

Lost/Stolen Devices

Problem:

The security risks to the enterprise associated with lost or stolen employee devices is nothing new, but the growing mobile workforce leaves these tools open to loss or theft. Due to lack of built-in enterprise server control and remote management, iPads and other tablets cannot be remotely wiped or locked by enterprise IT if the device falls into less than scrupulous hands.

Solution:

If a device is lost, stolen or compromised, solutions exist that allow IT managers to remotely wipe corporate files off the device. When it comes to iPads in the enterprise, it's best to consider a mobile security option that not only has trusted experience in the enterprise space, but also has a proven track record integrating Apple® devices with Windows® servers.

While theft and loss of employee devices cannot be completely avoided, both mobile file management and mobile device management solutions go a long way in protecting corporate assets. The best solutions also allow IT to configure specific access based on the enterprise's unique policies, like those that integrate with Active Directory, and to turn off or on the user's ability to open, print, or email a file, and more.

> *"Security experts agree most of the threats to mobile devices come in the form of people losing their devices or having them stolen. Rather than dealing with malware, the primary challenge for enterprise mobile security is figuring out how to best manage the plethora of devices employees can bring on to the network."*
>
> *—eWeek.com, "Dealing with Enterprise Mobile Security," October 6, 2010*[3]

Open Wi-Fi and Public Hotspots

Problem:

Studies show that consumers (and hence, employees) are lax about mobile phone security.[4] A recent report from Juniper Networks states that Wi-Fi attacks are on the rise, as open connections give hackers easy access to social networks and email.[5] What's worse, many consumers are still not aware of the risks associated with public Wi-Fi networks, even those that appear as "closed" hotspots. For example, in April of this year, U.K.-based newspaper The Guardian set up a mock Wi-Fi hotspot in an airport and was easily able to obtain user information ranging from email passwords to credit card information.[6] The same article states that corporate information on smartphones could be just as easily compromised.

Solution:

What's an enterprise to do? Clearly, it's impossible to keep employees from using their smartphones and tablets in public – it defeats the innate productive purpose of the device. Mobile device management does allow for device provisioning and management tools as well as the ability to encrypt and password-protect applications and email/PIM solutions that reside in a proprietary container. However, MDM only goes so far, stopping at the ability to protect corporate files or assets that reside outside of the proprietary container which is absolutely essential. Hence, a solution that provides on-device corporate file security and permissions is required to protect assets and ensure both the device and network are protected. [7]

Malware and Viruses

Problem:

With emerging technologies comes new and evolved malware. Recent press regarding malware well-disguised as Android applications has brought this issue to the forefront of corporate IT mobile security concerns.[8] While iPad has yet to be a primary target of Trojan apps thanks to Apple's tightly-monitored app store, the device is not completely immune to viruses.[9] And, as the device gains popularity, so will its propensity to be a target for malicious attacks.

> *"If you own an Android® phone or iPhone®, you're 2.5 more times likely to accidentally download malware today than you were in January."*
>
> *–TGDaily.com, "Mobile malware explodes in first half of 2011," August 4, 2011*[10]

Solution:

Enterprise IT cannot prevent employees from downloading mobile applications that might track critical information and eventually gain access to indispensable assets. They can, however, protect those assets on the server and network side through encryption for file transfer and storage on an employee's device. Designed to integrate with existing corporate security infrastructure, mobile file management solutions provide these features along with centralized control to give enterprise IT the added ability to remotely wipe an employee's MFM app should it become compromised.[11]

Corporate Policies to Address Emerging Technology Threats

Problem:

Unclear corporate policies to address new technologies while supporting employee benefits that come with the increasing consumerization of IT may not seem like a security threat, but according to recent reports, not having clear standards in place opens the door to risks.[12] Many enterprises are overwhelmingly supportive of employee choices when it comes to the variety of devices and applications available to them to boost productivity. Yet the same companies have been slow to adopt corporate policies that address the specific threats that these emerging technologies bring into the workplace.

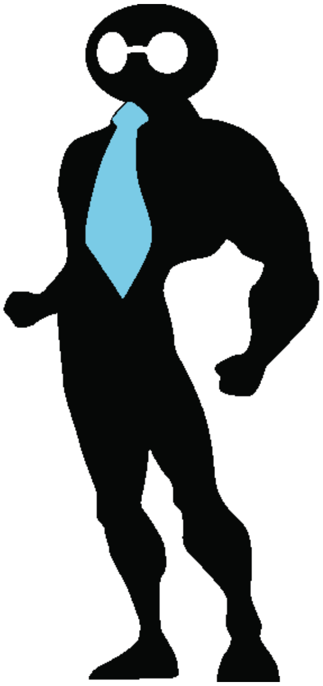
Solution:

Ensuring the integrity of corporate assets begins with clear, well-communicated policies and standards. While such measures can't do much in the way of preventing malware, they do set standards for employee responsibility and accountability—as well as awareness—when it comes to accessing, sharing, storing and transferring critical files on employee-owned or corporate-provisioned devices. Simply having a policy in place that forbids unsecure, consumer-based applications for the transferring of corporate documents—or sending it to oneself via email without encryption—is a basic, yet essential step employers can take against emerging mobile security threats. Secure mobile file management solutions allow the enterprise to provide the appropriate access to their mobile users. As an added measure, it is recommended that organizations adopt a mobile device management strategy for device provisioning, management and email protection.

ENFORCING POLICIES WITH MOBILE WORKERS

In the May 7, 2011 issue of InformationWeek, reporter Michael Finneran states,

"You can't secure a mobile workforce without a well-thought-out policy. And you can't expect people to adhere to policies that aren't enforced." [13]



Conclusion

Emerging technologies that benefit the mobile workforce are a boon for enterprise productivity. Ensuring that the security threats these technologies bring with them do not compromise critical corporate assets is all about empowering IT departments, as well as employees, with tools that address security concerns, yet give employees the access and usability they've come to expect.

Tablets and smartphones are in use in many environments ranging from retail to healthcare,[14] and their adoption is sure to continue to rise. Solutions exist that meet the very real needs for employee mobile file access while maintaining enterprise compliance and control. Such solutions easily install on existing corporate file servers in less than 10 minutes and feature instant integration with the device, so that IT can extend existing user policies and file permissions to the mobile device immediately.[15]

About Acronis®

Acronis® is leading the next wave of data availability, accessibility and protection solutions to simplify today's complex IT environments. Acronis technology enables organizations of all sizes to manage the always-on anywhere data access demands of users, reducing risk against the loss of valuable corporate data, and controlling management and storage costs. With proven technology for data migration and disaster recovery for physical, virtual and cloud environments, and secure enterprise file-sharing and synchronization regardless of type or platform, Acronis is enabling organizations to embrace new IT strategies and options such as BYOD and Mac in the enterprise. For additional information, please visit www.acronis.com. Follow Acronis on Twitter: http://twitter.com/acronis.

1. http://www.tmcnet.com/channels/mobile-device-management/articles/215991-employee-use-demands-mobile-device-management.htm

2. http://www.wired.com/threatlevel/2011/05/dropbox-ftc/

3. http://www.eweek.com/c/a/Security/Dealing-With-Enterprise-Mobile-Security-855336/

4. http://www.cnn.com/2011/TECH/mobile/03/28/survey.security.mashable/index.html

5. http://www.webpronews.com/mobile-device-security-threats-at-all-time-high-2011-05

6. http://www.guardian.co.uk/technology/2011/apr/25/wifi-security-flaw-smartphones-risk

7. http://www.grouplogic.com/resource-center/white-papers/enterprise-security-with-mobilecho-form.html

8. http://www.eweek.com/c/a/Security/Android-Most-Targeted-Mobile-Malware-in-Q2-2011-McAfee-128399/

9. http://www.geek.com/articles/mobile/ios-has-10x-more-security-holes-than-android-but-its-still-safer-says-symantec-20110628/

10. http://www.tgdaily.com/security-brief/57684-mobile-malware-explodes-in-first-half-of-2011

11. http://www.networkworld.com/news/2011/052311-grouplogic-mobilecho.html

12. http://www.thesecurityblog.com/2011/06/how-businesses-and-users-can-improve-mobile-security/

13. http://www.informationweek.com/news/mobility/business/229402924

14. http://www.smartgorillas.com/?p=5507

15. http://www.grouplogic.com/enterprise-file-sharing/ipad-file-system/

For additional information please visit http://www.acronis.com

To purchase Acronis products, visit www.acronis.com or search online for an authorized reseller.

Acronis office details can be found at http://www.acronis.com/company/worldwide.html