In this paper, you will learn about the rise of empowered tablet and smartphone users, and the additional risks of data leakage and loss which their behaviors invite. You will discover how the IT security industry is responding, and where it’s falling short. And you will then find out how emerging innovations in virtualization are successfully taking on the specific threats which mobile devices present, with the potential to usher in a new era of information/data assurance.
Contents

1. Mobility Brings New Cybersecurity Concerns ................................. 4
2. Industry Response Remains Incomplete ....................................... 4
3. Essential Assets for Protection .................................................. 5
4. Empowered Mobile Users Invite New Risks .................................... 5
5. Falling Short of Complete Assurance ........................................... 6
6. Virtualization Solutions Help Resolve the Security Equation ............... 7
7. Raytheon Trusted Access Mobile ................................................ 7
8. A Comprehensive Mobile Security Strategy for the Present... .............. 8
   Promising Development for the (Very Near) Future

References

https://blog.lookout.com/blog/2011/03/01/security-alert-malware-found-in-official-android-market-droiddream/


http://blog.malwarebytes.org/mobile-2/2013/09/obad-trojan-found-in-fake-google-play/

http://mobithinking.com/blog/mobile-web-penetration


http://www.gartner.com/newsroom/id/2466615

http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD

http://www.slideshare.net/citrix/citrix-mobilityreportbyod2014

http://www.navisite.com/download-daas-survey

http://www.itbusinessedge.com/cm/community/features/interviews/blog/employees-bypassing-it-as-byod-takes-hold/?cs=50441
Mobility Brings New Cybersecurity Concerns

In 2011, a malware attack named DroidDream infected more than 50 popular mobile applications – including business tools such as a file manager, scientific calculator and advanced currency converter – to take control over devices and steal sensitive data. Then, in 2012, news reports revealed that “Red October” had been stealing hundreds of terabytes of sensitive data from mobile devices and other entry points, impacting business and government users in 36 nations, including the U.S., Russia and Iran.

Last year, a Trojan named Obad created a bogus Android Google Play store to launch botnet-enabled malware distribution on mobile devices, granting itself extraordinary administrative privileges which were extremely difficult to undo. In fact, Kaspersky Labs described Obad as the “most sophisticated Android Trojan yet.”

These and other incidents underscore a sense of urgency when it comes to mobility, security and the enterprise. And, make no mistake about it, the Mobile Age has just begun: About nine of ten Internet users will access the Web from smartphones, tablets or other mobile devices by 2017, up from about three-quarters of users in 2013, according to eMarketer.

But security remains a pressing source of concern. The rate of growth of new mobile malware primarily targeting smartphones and tablets is far outpacing that of PC-based attacks. As using personal products for work purposes continues to build momentum this trend is sure to continue. Thus, organizations face new exposures in terms of data leakage and loss. For these organizations, sensitive and/or proprietary data and information represent their most precious asset. In the wrong hands, the fallout from an incident in which device-contained data and information are compromised can be crippling.

In this paper, you will learn about the rise of empowered tablet and smartphone users, and the additional risks of data leakage and loss which their behaviors invite. You will discover how the IT security industry is responding, and where it’s falling short. And you will then find out how emerging innovations in virtualization are successfully taking on the specific threats which mobile devices present, with the potential to usher in a new era of information/data assurance.

Research demonstrates that threats impacting smartphones, tablets and other mobile devices are rising quickly. User behavior is adding to the risk of data leakage and loss:

- The appearance of new mobile malware – almost exclusively focusing on the Android platform – grew by 33% over a six-month period last year, while new malware targeting PCs remained nearly flat.
- 83% of organizations indicate that mobile devices overall create a high security risk.
- 60% of employees admit to engaging in some form of risky behavior on the devices they use for work, and one-third download malicious apps, documents or other files.
- 32% of all mobile threats are launched for the primary purpose of stealing information.
- 73% of organizations are either “very” or “extremely” concerned about loss of their data on mobile devices.

Sources: Cisco, McAfee, Symantec, Webroot

Industry Response Remains Incomplete

To combat the growing concern of security around mobile data access, industry has introduced an assortment of technologies – walled gardens, application white listing, data wiping and similar concepts with limited success. Mobile Device Management (MDM) has gained perhaps the most attention, albeit, MDM is somewhat mislabeled as a security solution given that its main purpose is device provisioning, management and optimization. Nevertheless, the allure of MDM has reached a zenith; there are nearly 130 vendors in this space. Not to dilute their utility, but surely differentiation and manageability would be difficult considering the vast number of MDM offerings and the diversity of devices for which they’re acquired.

Upon further review, it’s obvious that the sheer volume of devices and their variants demand greater protective assurances than these responses can provide on their own. These solutions are designed with a sole purpose: to ensure that data on the device is not misused, stolen, lost or leaked. The data, however, still resides on the device.
The same thesis applies to secure containers – another application-layer solution which purports to keep apps and data within a designated area at a device-centric level. True, containers offer a better approach than MDMs, but they still do not establish the assurance needed for private, sensitive or classified information as they, too, are focused on the device. Any concession at the OS level below the stack of the device will blow apart the data.

Ultimately, mobility solutions must protect the data first and foremost, as opposed to the device.

Fortunately, there are emerging, virtualized technologies that directly address this need, to secure data as is resides in the enterprise. As a result, devices are treated as just another endpoint, which is what they are. It’s the data that really matters.

**Essential Assets for Protection**

First, let’s examine two key assets which any IT security effort seeks to defend: data and applications.

**Data.** Practically every organization on the planet is a data-driven one: The digital universe is doubling every two years, and will equate to 40,000 exabytes by 2020, according to IDC. (A single exabyte of storage can contain 50,000 years’ worth of DVD-quality video.)

But not all data is created equal. Each individual piece is defined by its attributes. Beyond the meaning and the use of the data, the attributes can define sensitivity levels, access controls and, in military/intelligence circles, clearance classification (e.g. “Unclassified,” “Sensitive But Unclassified,” “For Official Use Only,” “Secret” and “Top Secret”). This has led to formal efforts in data tagging, along with usage attributes. The higher data sensitivity requirements dictate that certain agencies – particularly those within the Department of Defense (DoD) and Intelligence Community (IC) – ensure physical separation and put in special safeguards for the storage, access and transfer of data.

Due to compliance mandates, private industry deals with similar dynamics more frequently these days. Regulations such as HIPAA and PCI speak to the oversight of sensitive information such as Personally Identifiable Information (PII). Additionally, any corporate information – like disclosures related to financials and the like – merit the same attention.

**Applications.** The Mobile Age gave us the very term, “apps.” When we hear the word, we picture tech tools which value ease of access to information from anywhere by anyone, regardless of security considerations. This is fine for consumer apps (at least until something goes wrong); but not for enterprises, especially when systems running mission-critical tasks are exposed. (Because by the time “something goes wrong,” it’s too late.) Web-based access further complicates the challenge. Nevertheless, with the right amount of policy enforcement, ease of app usage can still be preserved.

The safeguarding of data/information and apps for remote users introduces difficult questions:

- How different are the needs for the protection of data/information and apps today than they were in the pre-mobility days?
- Is securing the end-point the most effective way to fortify sensitive information?
- Are attributes and usage requirements the same for all data, regardless of the degree of sensitivity?

**Empowered Mobile Users Invite New Risks**

A profound cultural shift among virtually all private organizations and government agencies is further complicating the topic. In decades past, senior management and/or the IT department dictated to employees the kind of machines they would use, right down to the make and model. They would determine which software tools were allowed and which were prohibited.

Well, mobility and its derivative – the Bring Your Own Device (BYOD) phenomenon – coupled with the rising tech sophistication of the general public – has changed this dynamic in a hurry. The mass consumerism of technology has shifted the power of choice to everyday users. They’re confident that they know what devices and apps will maximize productivity. Frankly, employees can “get their own way” on tech deployment because organizational leadership cannot ignore the vast, business-benefiting outcomes. IT, in turn, is transitioning into a somewhat resigned, “can’t beat ’em, join ’em” stance.

Unlike alternative technology adoption processes in which significant vetting takes place before any acceptance/deployment, IT personnel are rushing to understand and react in some manner, without stifling the adoption surge. These devices are updated frequently with respect to software, OS, etc., making it difficult to stay on top of it all. Frankly, this can keep the tech department awake at night: What if a device with sensitive information is stolen? What if users visit malware-infected sites and links? What if they download highly suspect content, opening the door to a network attack?
What's more, compared to computing products of just a few years ago, devices today pack a big punch, capabilities-wise. Time magazine once famously described the standard smartphone running on an Apple iOS or Google Android operating system as having "more computing power than Apollo 11 when it landed a man on the moon." This means they're quite valuable, if not vital to accomplish mission-critical jobs. But this increases their profile as targets of cyber threats. When such a device is introduced into an enterprise, the primary concern is security – especially as it relates to safeguarding information which may be sensitive, classified and/or proprietary.

Device-centric solutions are not enough to assure a high level of security when sensitive or classified data is accessed on the device.

We consider MDM and the aforementioned approaches as a decent start. But with the challenges of potentially vulnerable sensitive corporate data on so many different devices, organizations are better served by protecting data at the source instead of securing the plethora of devices.

HTML5/responsive Web design (RWD) has emerged as a mobile-development option, as 43% of U.S. IT managers say they've adopted both, according to research from Forrester. However, many IT managers have concluded that mobile HTML5 apps are slower than native mobile apps, with delayed updates and bugs and an overall excessive amount of time spent on testing and fixes, according to a published InfoWorld report. Additionally, web apps fall short where rich user experience and response are required. Ultimately, HTML5 and IT managers feel that it's best for small subsets of apps, such as internal lines of business, according to the InfoWorld report.

Beyond security concerns, there are many logistical issues presented by MDM, containerization and the other solutions. BYOD has unleashed a Pandora's Box for organizations, as IT departments and leadership seek to establish usage policies, which employees resist. They don't feel the tech department and managers have a right to dictate what they can and cannot do with their devices. Who owns the device anyway – the company or the users?

Then, there are the immense burdens placed upon IT administrators. Devices and operating systems continue to proliferate and admins can't keep up – again, because they are deploying device-centric tools, not data-centric ones.

This sets up a perfect storm of troubling questions which options like MDM and containerization fail to sufficiently answer: How many devices can an enterprise manage before it becomes too complex? Given the fundamental change the mobility paradigm brings to the workplace and lessons learned from end-point security, is it time for a different approach? Most importantly, is the assurance established by these solutions enough and do they accommodate all types of data – unclassified and sensitive – in all types of situations?

Of course, the only 100% certain way to address every potential problem – including the elimination of data leakage and loss – is to entirely ban the storage of work-related, sensitive data or apps on devices. But that isn't going to happen. As the saying goes, the genie is out of the bottle and he's not going back in.
Virtualization Solutions Help Resolve the Security Equation

In the Windows workstation world, there’s Virtual Desktop Infrastructure (VDI) software, which separates the desktop environment and apps from the client used to access it. There are many advantages associated with VDI, including reduced administration, enhanced security and decreased power usage. Users connect to their Windows environment, which resides securely in the cloud as opposed to the desktop. If anything happens to the desktop, critical or sensitive data is not compromised.

In other words, virtualization is about safeguarding data, not the machine. VDI is quickly gaining in terms of public and private-sector deployment, as Gartner estimates virtual desktops account for 40% of the entire PC market.

But VDI in and of itself falls short in terms of its usefulness within the mobile environment. Primarily, desktop applications are optimized for a keyboard-and-mouse environment while mobile devices sport more interesting options.

But the concepts behind virtualization need not be lost altogether. By virtualizing the native mobile apps themselves and securely redisplaying them on a tablet or smartphone, these technologies can be optimized for the mobile world. This is referred to as Virtual Mobile Infrastructure (VMI). VMI takes advantage of virtualization and redisplay technology to extend access to sensitive information from a commodity device without elevating risk.

VDI attempts to make the mobile transition. But it can’t because desktop apps are designed for Windows environments. To receive the necessary mobile support, executive leaders must turn to VMI, protecting not only public but sensitive/classified data at the source as opposed to the device. (VMI, like VDI, is safely secured in the cloud)

There are additional advantages: Those logistical complexities mentioned previously disappear. IT admins don’t have to oversee an ever-increasing number of devices and operating systems. With VMI, they focus on the data residing in the cloud. As for those devices, they are just endpoints, nothing more. Administrators streamline user/device registration while publishing and managing apps from a central point of management. Cost savings are considerable, as you won’t have to target multiple platforms for the same app.

VMI is BYOD-friendly too. Since data and apps never reside on the device, there is no need for extensive legal policies to address data wipes and separation of personal and mission-intended apps.

VMI controls access across the mobile continuum – from the device to the back-end through policy enforcement customized for the enterprise. Enterprises decide who gains entry to what apps and data, based upon not only their identity but other factors such as location. It does not replace an organization’s MDM solution, nor is it dependent on a particular MDM product. It can function as simply another part of a mobility management ecosystem.

Raytheon Trusted Access Mobile

For organizations requiring access to sensitive data and applications at either single or multiple classifications, Raytheon enables secure access and interactions with data from any location on mobile devices. To advance beyond container and MDM-based protection/remediation technologies, Raytheon virtualizes native mobile and other types of applications in a secure infrastructure and leverages redisplay technologies for user interactions, thus alleviating concerns of data loss, theft and compromise.

Specifically, Raytheon has developed Trusted Access Mobile, a VMI platform with a secure-access framework and a virtual mobile-device infrastructure. The framework manages identity tokens, secure network communications, access policy enforcement and contextual awareness, with a virtual mobile app management and hosting service which end users access via redisplay.

Sensitive data and apps are secured on the back-end. The mobile user is granted entry to protected resources hosted on the virtualization platform after authentication. Once authenticated, the user is allowed access to resources based on access control dictated by policy that can be applied based on contextual awareness.
Virtual mobile apps are protected on the device, where they are immune from any tampering or exploitation that might occur on a compromised edge device. Enterprise data is accessed by the virtual mobile apps only, so sensitive and proprietary data never leave the protected network. There is no potential for a malicious app on the edge device to opportunistically scan the enterprise network.

As with desktop systems, Trusted Access Mobile allows for the enterprise computing system to audit and detect questionable user behavior. The virtual mobile device runs on enterprise-owned hardware in the back-end and is owned by the enterprise, so there are no legal or technical impediments to deep audit/detection instrumentation being applied to the device.

In summary, here’s why organizations need Trusted Access Mobile:

- It’s **ideal** for Bring Your Own Device (BYOD).
- It **co-exists** with existing MDM and Mobile Application Management (MAM) solutions.
- It **enables** customers to conduct confident and cost effective collaboration.
- It **provides** access to sensitive, confidential, or proprietary data.
- It **protects** against data loss and compromise prevention.
- It **allows** access to native, desktop and web apps.

**A Comprehensive Mobile Security Strategy for the Present... A Promising Development for the (Very Near) Future**

We want to stress that we are not criticizing current technologies discussed in this paper. Many are good at solving some of the problems. But we must take the next step forward, to always think about protecting the data first, as opposed to the device.

That’s where VMI is emerging as a preferred technology approach. It establishes the highest standards of security, while allowing mobile users the flexibility they seek. They’re able to deftly manage the mix of sensitive and non-classified data/information.

Through these technologies, organizations will have every opportunity to deliver the best of both worlds: Ease of user function, the capability to communicate in real time, regardless of clearance, and a fully secure mobile environment. That’s what a “protect the data” strategy versus protecting just the device – is all about.

**Written by Ashok Sankar, Raytheon Cyber Products**

Ashok Sankar is Senior Director, Product Marketing Strategy at Raytheon Cyber Products, a technology and innovation leader specializing in defense, intelligence, civilian, and commercial markets throughout the world. Its product, Trusted Access Mobile provides defense-grade security to protect critical, sensitive, and proprietary data. It is fully compatible with solutions from leading vendors such as VMware® and Citrix®.