SYNOPSIS GROUP

Whitepaper: Mobile Devices - How To Secure Sensitive Data.

Date Created: 27th November 2019

Version Control:

Version	Description of Changes	Date	Author(s)
Draft	Creation of document	27/11/2019	Nardus Schroeder

Contents

Mobile Devices - How to Secure Sensitive Data

Introduction

Sales of mobile devices continue to skyrocket: IDC reports that 2018 worldwide shipments of smartphones reached 1.49 billion units - up 2.1% from the 1.46 billion units shipped in 2017. And although tablet shipments globally are seeing a slight decline, 128 million units are expected to shipped by the end of 2018.

Smart mobile devices are now ubiquitous in the workplace, and many employees are bringing their own (BYOD) to work. Add social networking to the mix, and it's clear that organisations face a host of new challenges when it comes to safeguarding sensitive information.

In this short white paper, we:

- Examine the risks presented by increased mobility in the workforce
- Look at the main options for protecting sensitive data on mobile devices, and
- Discuss their pros and cons with a clear focus on practical issues.

The genie's out of the bottle

"IT Security Trends: Mobile security concerns tops the list. "

That's the heading of a report on a survey conducted by Search Security. However, a June 2012 survey by Gartner found that 90% of US enterprises have already deployed mobile devices (mostly smartphones), and almost the same number said they planned to deploy media tablets in the same year. Gartner Director Chae-Gi Lee said 'Enterprises should look to "mobile enable" their IT infrastructure for employees to meet the growing demand for mobile device use in the enterprise IT environment.

Gartner tells us that 'BYOD is here and you can't stop it,'5 and warns of more problems for IT security staff and corporate helpdesks. Somehow, your IT team is expected to take care of these problems.

". we saw an increase in Android malware detection by around 20%... Even as ESET observed the largest spike in the first half of 2016, we are nowhere near saying that this threat will disappear anytime soon." ESET CTO 2017

The real world

According to ITBusinessEdge, these are the main mobile device risks for most organisations:

- The location of data on mobile devices is not tracked.
- Encryption and authentication are not enforced.
- Too many staff have unlimited access to business information.
- Mobile devices aren't checked for secure configuration.
- No acceptable use guidelines are enforced, and staff are not being educated.

That's the point: IT teams already have too much on their plates, and so some tasks are just not being done. Cyber criminals have already picked up on this vulnerability; with mobile devices operating outside your firewall, they're much easier targets.

An added problem is that most AV (anti-virus) apps aren't very good at detecting polymorphic malware, as US researchers showed recently. 'As long as antimalware tools continue to use content-based signatures,' lead researcher Yan Chen concluded, evading them is really easy.
A survey conducted by the Cloud Security Alliance found that only one security problem ranked higher on the scale than mobile malware: data loss from lost or stolen devices. This isn't surprising when you consider just how many mobile devices are lost every year:

- 113 cell phones are lost or stolen every minute in the U.S.
- About 12,000 laptops are lost each week in US airports alone.
- 10,000 mobile phones left in London cabs every month.

Some 60% of lost or stolen devices contain sensitive and confidential information, according to a Carnegie Mellon study, and it's serious, because we're talking about business data, passwords, PIN numbers and credit card information. While it may be an inconvenience for a user to lose a mobile device, for your organisations it's serious exposure if the device has access to your corporate network. Mobile computing is profoundly changing the way we work, so it must also change the way we safeguard sensitive corporate information.

Is EDM the answer?

"It's no surprise that Email Device Management (EDM) solutions are proving popular; they can wipe data from lost or stolen mobiles. However, EDM systems are not the solution, according to InformationWeek: 'mobile data and mobile operating

systems present a different security challenge from PCs, which is why just implementing EDM software won't solve Its BYOD and mobile management headaches."

The article also refers to a survey of CIOs, half of whom say their companies don't plan to deploy EDM at all.

"A big reason for BYOD is to get out of the equipment business." said one CIO. "If you implement EDM, you are back in the equipment business."

In fact, it's a whole new network of mobile equipment, and that network is increasingly controlled by the user, not by you.

The issue isn't just the equipment; it's the extra IT support it requires. In a BYOD environment, 'the complexity of this task is magnified many times over,' says Network World, 'because companies are allowing employees to use their own personal smart phones and tablets for business purposes.
Software updates, new versions and features add more complications, both for set-up and ongoing maintenance. EDM solutions also require:

- Network, application and user-level monitoring Access, incident, problem and request management
- Remote monitoring and management of users, devices, network and applications
- Compliance tracking (to ensure users are adhering to acceptable use policies) Cost management.

"...just implementing EDM software won't solve Its BYOD and mobile management headaches".

What about DLP?

DLP systems can be very effective in safeguarding sensitive information, but they need to be set up correctly, and that's only after measurable outcomes have been defined. Careful preparation is essential for DLP, focusing on issues like:

- *Deciding which data needs to be tracked by DLP*
- *Classifying the information and locating it*
- *Setting rules for document circulation and handling*
- *Creating and enforcing security policies*
- *Ensuring that privacy laws in different jurisdictions are observed*
- *Defining the success criteria of the project.*

DLP systems can also be high maintenance, depending on how dynamic or static the data in your organisation are. This can have a big impact, especially on the resources you'll need to find for DLP projects, at both business and IT levels.

Many valuable lessons have been learned in the last few years and, if you're planning a DLP deployment, this document from Deloitte and Symantec covers most of them: Avoiding DLP Pitfalls - A Discussion of Lessons Learned.

What about VDI?

The extra burden for IT teams could perhaps be lightened by virtualisation. VDI (Virtual Desktop Infrastructure) offers simplified desktop management, reduced costs for desktop hardware and centralized management of applications and users, and can be deployed in several ways:

- VDI based on in-house servers enables the data accessed by users to stay on your servers behind the firewall. The problem is you'll need more investment in server hardware, storage and network infrastructure, which may cancel out the savings on PCs.20
- VDI based on a cloud computing platform (also known as DaaS – Desktop as a Service) gets around the equipment cost issue, but adds the extra risks associated with storing your data in a hosted, multi-tenant environment.
- VDI can also be used as a platform to deliver virtual desktops to a variety of devices (from laptops to tablets and smart phones), providing mobile workers with secure access to data and applications from any device.

The third option initially sounds good but falls down in practice:

"Trying to use VDI on touch screens can be a nightmare," says TechTarget.

The problem is that VDI was designed for PCs with screens, keyboards and internal memory, but no storage facilities. Therefore, VDI doesn't work well on smart mobile devices including tablets. To use a remote desktop, tablet users need keyboards and mice just as for their PCs and, understandably, that's not an acceptable option.

Benjamin Robbins from Enterprise Mobility Consulting Group Palador told TechTarget. "Remote desktops try to cram an old technology into something new … the more we use mobile devices, the quicker they mature in features and the more they evolve in functionality -- and the sooner remote desktop will fade into the past."

In 2012, Gartner reported that VDI adoption rates had plateaued at around 10% because virtual desktop performance still didn't compare to that of a traditional PC.

"Trying to use VDI on touch screens can be a nightmare" TechTarget December 2012

Locking users down won't work

So EDM, DLP and VDI have some limitations, so how can you secure mobile devices? One thing is for sure, if you try to lock down your controls, you'll run into user resistance. They'll look for ways to get back their flexibility or get around your controls, and you won't know which or how.

They can:

- Create Google apps accounts to work on or share documents more easily
- Auto-forward work emails to their Gmail accounts for easier mobile access
- Use Gmail when they want to communicate outside your control zone

- Forward emails to Gmail when travelling for easier mobile access
- Forward email messages to Gmail when they're about to resign.

If you don't want to foster these practices, the ideal solution to protect sensitive data on mobile devices can't be onerous for users, can't interfere with how they work and must work on the wide range of devices they're using. Of most importance, though, is that you must focus on protecting what is actually sensitive: the data not the device.

80% of survey respondents said they used their mobile devices for corporate email
2012 Dimension, Research Survey

Address the real problem – email

Sensitive data held behind the firewall is not exposed to high risk; it's only exposed when it's moved, and email is the primary method of moving and sharing information, as it is corporate communication. As we saw, 80% of mobile device users use them for email24 so it's the obvious place to focus on protecting sensitive data.

The easiest way to do this and avoid the evasion practices we mentioned, is by email classification; that is, adding protective markings to emails (and documents) according to their sensitivity. It's because it's easy to do and works that countless government agencies across the globe, including those holding critical information, have adopted email classification.

It enables:
Prevention of accidental or deliberate leakage of sensitive information
Protection of valuable Intellectual Property and corporate information assets
Limited legal liability and exposure
Increased security awareness across whole organisations
A low cost solution that's simple to deploy, configure and manage.

So how does email classification work in the mobile world? The most obvious answer is to stop sensitive information being moved to mobile devices.

To achieve this, some solutions deploy a 'containerisation' model, where emails containing sensitive information are 'sand-boxed' for inspection by the mobile device user. Initially this might sound promising until you look at the impact: containerisation complicates the operation of the device, it requires installation of more applications on the device, and it has a noticeable impact on device performance. If you're looking for the reverse, and for users to comply rather than evade, this may not be the answer. Keep it simple and cost effective.

A simpler way to prevent sensitive information moving to mobile devices is to filter the email traffic before it reaches the device, that is, between the email server and the mobile device, and this can be achieved even without email classification. In fact, you can pre-set your filtering rules to detect a wide variety of data types, depending on your business and situation, such as:

- Numeric sequences (e.g. credit card, social security, tax file numbers)
- Defined keywords (e.g. sales figures, customer database)
- Attachment names and extensions (e.g. Excel spreadsheets)
- Security classifications in subject lines or in the body of a message (e.g. Confidential)
- Any attachment (e.g. nothing to be attached).

Using this approach, the mobile device user gets to know about the message, but doesn't receive it or its attachment. When sensitive corporate content is detected in the email, the mobile device user is emailed that the original message has been delivered to her corporate desktop (behind the firewall). If personal or confidential information is detected in the original message text, that portion of the message can be redacted, so nothing of sensitivity will reach the device.

A simple solution like this, called Mobile Email Management (MEM), can address the security risk associated with mobile devices for a fraction of the cost and complexity of other solutions. MEM can be used with any email classification system or with none; it operates before the message reaches the device and it focuses just on sensitive email traffic which is only 5-10% of the total.

That means your users won't miss any messages, they won't experience reduced performance or operation of their mobile devices, and they might only be aware of MEM because it's your policy. If they're not impacted by MEM, they'll be less likely to look for ways around it too.

Mobile Email Management can address the security risk of mobile devices for a fraction of the cost and complexity of other solutions.

Get the business benefits

Solutions like MEM unlock the productivity gains and flexibility promised by mobility at the start; that is, users can deal with 85-95% of their email traffic, and do it without the extra constraints of more complex solutions. Because these solutions deliver all emails to the mobile devices, they shift the security layer out to the device, so the user is the one impacted. This is a sure way to encourage them to circumvent the rules, even if it's just to please a customer, to take work home or to gain the flexibility their friends enjoy at other workplaces.

To achieve user acceptance and cooperation, you'll need to ensure simple operation and no (or very low) impact on work practices. To make it easy for the IT team too, you'll need low demand on technical support and easy integration with other IT systems. That's why the best MEM systems focus on:

- No effect on existing system configurations
- No need to change firewall rules or smartphone configuration
- Operation of all major devices in native mode (e.g. iPhone, Android, Blackberry, Windows Mobile, Windows Phone 7 and Symbian)
- No additional software or hardware
- Working with all mobile devices and rule sets, and adapting to new ones
- Working with the major email gateways (e.g. MSES 2007 and 2010)

- Working with ActiveSync so virtually any ‘new fashioned’ device will be accommodated
- Simplicity of installation and maintenance.

The bottom line

Absolute protection of sensitive data on mobile devices is probably not possible except within a custom-built, military-grade environment. As you probably can’t lock down your organisation or people in this way, yet seek the benefits mobility offers, you’ll probably accept mobile devices and the risks they entail. That said, you can mitigate the great majority of the risk with a combination of tools at different levels, and email classification and MEM (Mobile email Management) are practical elements.

Another element in your protection, a vital one, is your mobile device user base. If an email classification system or MEM reminds users constantly of the sensitivity of the documents they’re handling, not only do you share the task of information security among the many, you can foster a healthy security-aware culture across the organisation as a benefit. A real win-win.