CASE STUDY
Intel® Core™ Processor
Mobile Computing
Healthcare

Managing mobile

Study shows managing Microsoft Windows*-based tablets as a PC offers greatest security benefit for the scenarios tested for bring your own device at Madrid Community Health Department

Servicio Madrileño de Salud
SaludMadrid
Comunidad de Madrid

Dirección General de Sistemas de Información Sanitaria
CONSEJERÍA DE SANIDAD
Comunidad de Madrid

"The study shows that there are solutions that can avoid the 'D' from BYOD standing for 'disaster'. Each organization can implement the solution that best aligns with its strategies."

Jose Manuel Laperal,
Head of IT at SERMAS
Chief of Group at Madrid Health Department for Planning and Coordination

Madrid Community Health Department, together with Intel and security expert Stack Overflow, assessed several mobile operating systems to analyze their device-management capabilities. The results will determine best practice for managing new mobile platforms which are now being deployed as a result of the CIT Mobility Plan from Madrid Community Health Department to support bring your own device (BYOD) and other mobility scenarios.

Challenges

- **Addressing BYOD.** Increasing numbers of physicians and other staff were trying to access the corporate network from their own tablets and smartphones
- **Maintaining IT security.** The strategy for accommodating BYOD and other mobility scenarios must also assure IT security and data protection

Solutions

- **Study.** Madrid Community Health Department carried out a study to assess the impact of BYOD from both technical and legal perspectives
- **Meeting user compliance.** They tested the effectiveness of three different mobile device management scenarios in meeting 18 key compliance statements

Impact

- **Good practice.** Managing Microsoft Windows* 8.1 tablets as a 'normal' PC was shown to meet all 18 compliance statements. Managing Windows 8.1 and Android* tablets with mobile device management (MDM) was only able to meet eight and 10 user compliance statements, respectively

Integrating BYOD

Madrid Community Health Department is the agency in charge of providing public health services in Madrid. Currently, it is going through a huge transformation, to optimize its resources and offer a more efficient health service for citizens.

In accordance with the Mobility Plan of Health IT Department, it needed to analyze BYOD across the whole organization and, in particular, for physicians in hospitals, who would like to access the corporate network through their own devices.

BYOD describes an environment where the employees bring their own smartphones and tablets to work, using them to access the organization's IT resources. There are many advantages to this strategy, including increased flexibility and greater productivity, but there are also inherent security and data protection risks.

Analyzing risk

Madrid Community Health Department wanted to objectively understand the risk it was facing from BYOD. It turned to its trusted technology provider Intel to arrange an analysis of the impact of BYOD from a technical perspective.

Intel called in local, independent security expert Stack Overflow to collaborate with Madrid Community Health Department's IT security manager and Legal team to draw up a list of 18 security requirements it needed to meet (table 1).

Requirement	User compliance statements
1	You will not be able to modify computer equipment and peripherals or connect to any other equipment outside the health department without written permission.
2	You will not be able to store or download data on the device.
3	You will only be able to access the Internet for professional purposes.
4	The information on your device will be backed up regularly.
5	All the information on your device will be encrypted.
6	You will not be able to access your professional applications (container) from outside the hospital.
7	Your passwords must: • Have at least eight characters - alpha and numerical with at least one special character. • Be different for your personal and professional applications (containers). After three failed attempts to enter your password, your tablet will be blocked for a short period of time.
8	You will need to enter your password each time you access an application.
9	You will be logged out after a period of inactivity.
10	You will not be able to access the professional container log record.
11	You should know that the IT department will carry out periodic checks of your professional activity.
12	You will be denied access to blacklisted URLs depending on your profile.
13	Your anti-virus software will be updated by your IT department.
14	You will not be able to deactivate your security software, which protects against viruses, worms, and so on.
15	You will not be able to install software.
16	Your device cache will not be able to store information relative to last addresses or documents accessed.
17	Your user profile and device must be recorded in the management tool by the administrator.
18	In case of theft, loss, or termination of employment, the data and corporate applications on your device will be deleted.

Table 1: Security requirements drawn up by Madrid Community Health Department's IT and Legal teams

Managing Windows* 8.1 tablets as a PC can offer less risk than other Windows and Android scenarios tested

Stack Overflow and Intel then assessed the capability of three different scenarios in assuring compliance with these statements:

- A tablet running a Windows 8.1 operating system (OS) managed by MDM
- A tablet running an Android OS managed by MDM
- A tablet running a Windows 8.1 OS managed as a normal PC

Managing with an MDM

MDM products, many originally developed to manage Android-based smartphones, have become capable of managing Android tablets. A tablet device running Windows 8.1 can also be managed with MDM.

Stack Overflow evaluated the management of Android devices with MDM as the management console. Of the 18 compliance statements, only 10 were fully met.

Jose Manuel Laperal, Head of IT at SERMAS. Chief of Group at Madrid Health Department for Planning and Coordination, explains: "The BYOD possibilities of the tablets running an Android OS, managed by MDM, are interesting but cannot be addressed by an organization without an exhaustive analysis of their risks and the implementation of solutions to mitigate them."

Figure 1 shows the results of the testing.

The study also evaluated the management of Windows 8.1-based devices with MDM as the management console. The tests showed that, under this scenario, of the 18 compliance statements only eight were fully met and five partially met. This shows that the Windows 8.1 OS nearly matched the Android OS in delivering the manageability features required under BYOD scenarios tested for user-owned devices.

While the Windows 8.1 OS is built on a mature codebase, Microsoft has only recently begun exposing the management APIs for use by the independent MDM vendors. Also, since most of these MDM vendors are focused on market segments where Android and iOS* are more popular, the capabilities required to fully manage Windows 8.1 tablets are still developing.

Managing as a PC

Finally, Stack Overflow analyzed the benefits of rolling out a tablet running a Windows 8.1 OS managed as a normal enterprise PC. This was shown to have a number of advantages:

- Existing IT infrastructure—such as PC management consoles, servers, databases, security tools, and Active Directory* metadata—is already in place and has been tested at production scale.
- Operational procedures are already in place and IT staff is experienced in the management of Windows endpoint devices.
- Software licensing for Windows devices is usually in place and the costs are well understood.

Another advantage, not listed above but clear from the assessment, is that Windows management tools are mature and fully-featured for managing a tablet as a normal enterprise PC.

This study by Stack Overflow and Intel shows that adopting and managing tablets with Windows 8.1 running as a normal enterprise PC can manage and cover most of the risks defined, provided the tablet is given to the employee by Madrid Community Health Department as a normal PC (figure 2). "It is clear that risk factors identified in the study can be mitigated using the appropriate tools and techniques," concluded Laperal.

Lessons Learned

"The study shows that there are solutions that can avoid the 'D' from BYOD standing for 'disaster'. Each organization can implement the solution that best aligns with its strategies," said Laperal.

Managing Windows* 8.1 tablets as a normal PC was shown to meet all 18 compliance statements identified. Managing Windows 8.1 and Android* tablets with MDM was only able to meet eight and 10 user compliance statements, respectively. From this we can conclude that the tablets running a Windows 8.1 OS offer the Madrid Community Health IT department greater flexibility, since they can be managed both with MDM and as a normal PC.

Find the solution that's right for your organization. View **success stories from your peers** and check out the **IT Center**, Intel's resource for the IT Industry.

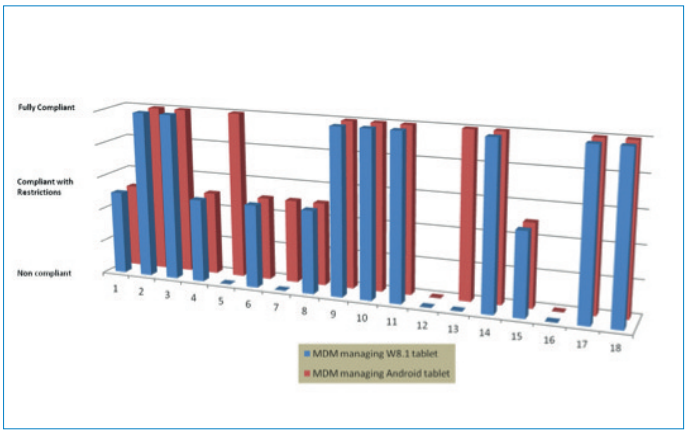

Figure 1: Managing Windows 8 and Android tablets with MDM

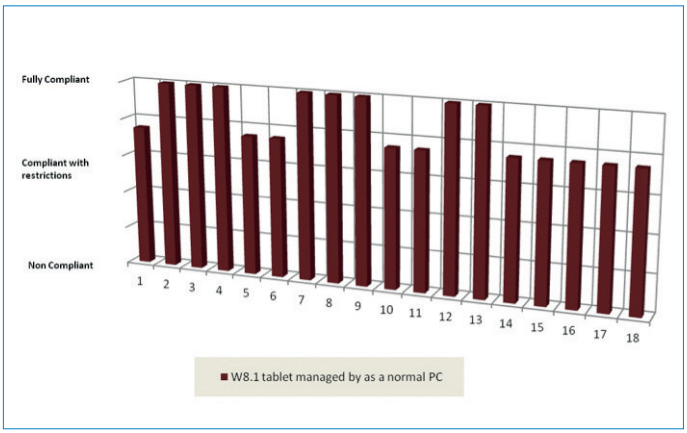

Figure 2: Managing a Windows 8 tablet as a PC

0115/JNW/RLC/XX/PDF 331867-001EN