Panasonic
BUSINESS

Addressing issues with Android in Enterprise

A Panasonic Toughpad Whitepaper

TOUGHBOOK TOUGHPAD

BUILT IN RISK?

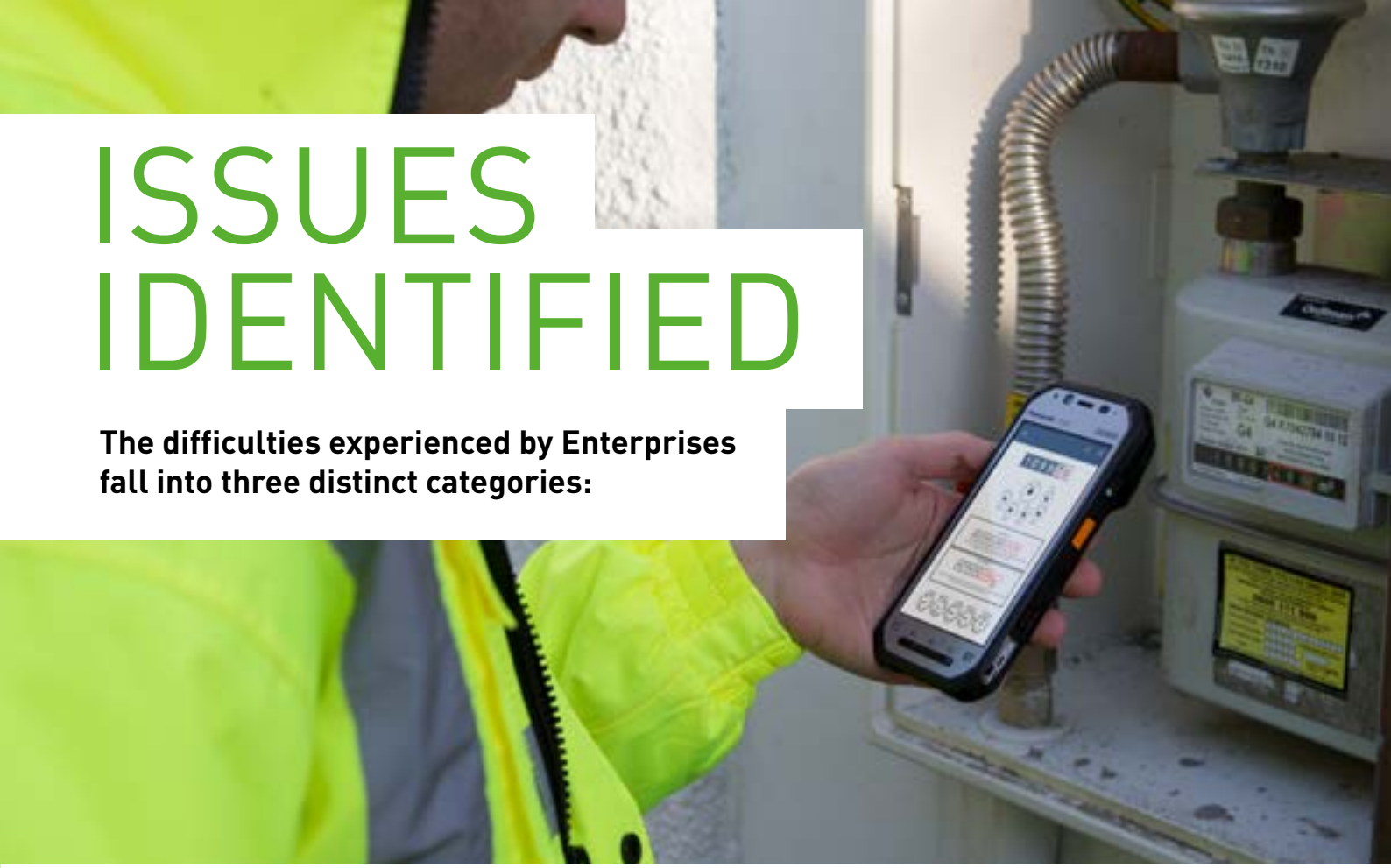
With the adoption of Android mobile devices in Enterprises growing, the attraction of increased flexibility, customisation opportunities and reduced deployment costs have been widely appreciated by many businesses. But early Enterprise adopters of Android handhelds and tablets are now also realising some of the long-term challenges surrounding the management and security of these devices.

An analysis of around one million Enterprise and business users in the US by security firm Duo Security has found that a staggering third of Google devices from its customer base of several thousand are still running versions 4.0 or below, which means they haven't been updated for several years.

1 IN 3 STILL USING 4.0 OR BELOW

Another 14 percent were stuck on Android 4.4.2 and nine percent on 4.4.4, which means that over half are using images that date back to the three years before October 2014 when Android 5.0 Lollipop made its appearance.

These staggering statistics underline the ongoing challenges of management and security that Enterprises face once Android handheld and tablet devices have been integrated into the workplace.



ISSUES IDENTIFIED

The difficulties experienced by Enterprises fall into three distinct categories:

Management

The ease of customisation of Android's open source software, along with the proliferation of mobile tablet and handheld device manufacturers, each with their own tweaked version of the operating system, has resulted in a wide variety of Android flavours in the Enterprise market. Although this flexibility and breadth of choice was initially viewed as a positive benefit for organisations, over time it has become an issue to effectively manage the devices.

The range of management challenges experienced include:

- **Difficulties in application roll-outs**
  A mixed estate of Android tablet and handheld devices creates application design and roll-out challenges leading to increased time and cost updating different device and OS groups. A lack of uniform Enterprise Mobility Management (EMM) certifications across the devices, for example, means that applications are more time consuming to deploy and not optimised for their devices.

- **Costly OS and application management**
  Firmware updates, system application upgrades (such as new versions of Chrome or new versions of customer applications, if present in system partition), driver fixes and patches can be a time consuming and costly challenge across multiple devices with multiple Android flavours.

Enterprise Security

Android devices require 3rd party security solutions to ensure that they are fit for purpose in the Enterprise world. A mixed estate of Android devices can make these solutions difficult to implement and challenging to maintain across a large Enterprise. The data security, costs and labour requirements of these security issues are often under estimated.

- **Bring Your Own Device (BYOD)**
  The implications of users using their own Android devices for work adds another layer of security complexity. It raises a wide range of security issues for the Enterprise to deal with including effective device and application management, partitioning of work and personal information, network and IT infrastructure protection from viruses and malware.

Knowledge

The issue of effective management and security of Android devices in the Enterprise is compounded by the fact that there is still a lack of professional knowledge and understanding around Android Best Practice in the Enterprise. This is mainly as a result of the short time that Android has been operating in the Enterprise and an Enterprise IT community that was brought up with and used to dealing with a Microsoft environment. However, until this knowledge becomes more widely spread and effective, it is important to establish Android best practice for purchasing, deploying and managing Android handheld and tablet devices in the workplace.

ANDROID FOR ENTERPRISE: **A CHECKLIST FOR SUCCESS**

Customisation to meet your business needs

Manufacturers should offer Enterprises the opportunity to customise the Android OS to suit its business requirements. A customised OS can help provide a customised user interface with improved signal quality, power management, and security options, alongside pre-installed applications, settings and company logos.

Peace of mind security

Your device manufacturer should certify 3rd party security solutions to enhance device security. All Android models should be offered with the opportunity to pre-install 3rd party security solutions. These solutions can help to implement strict password control, multi user profiles with different security policies, administrator authorised applications and administrator defined external interfaces, such as micro USB and Bluetooth.

A resource of Android Enterprise expertise

Finally, your device provider should be a resource of Android expertise for the Enterprise to call upon. With Best Practice recommendations and documentation, the device provider should be a partner in helping your Enterprise to get the very best from the flexibility of Android whilst ensuring your mobile devices are secure and can be effectively managed.

Ease of management

By owning and maintaining the Enterprise's customised version of the OS, your Android device manufacturer should be able to offer firmware updates Over the Air (FOTA), including security patches, system application upgrades, driver fixes and patches.

In addition, your manufacturer should provide the Enterprise with the opportunity of using a policy management tool for firmware updates. This Advanced FOTA service allows businesses to manage their own FOTA operations, such as to decide when and which policies regulate OS updates, and would provide some Mobile Device Management (MDM) and inventory management features. It should also include Software Component Management Object (SCOMO) functionality. This allows businesses to manage software on a remote device, including installation, uninstallation, activation and deactivation of software components over the air.

Finally, your manufacturer's devices should also be certified by prominent EMM vendors. EMM certification benefits include applications optimised for devices. Models can also be pre-installed with EMM clients to make roll-outs simple.

COMPASS

COMPLETE **A**NDROID **S**ERVICES AND **S**ECURITY

Panasonic COMPASS offers businesses everything they need to deploy and manage their rugged Android tablets and handhelds securely. It is designed to give businesses the confidence to take advantage of the flexibility offered by an Android operating system with the reassurance that Panasonic's devices are business-ready for applications, management and security. Panasonic Toughpad currently offers a range of market-leading, Android rugged tablet and handheld devices with 4, 5, 7 and 10 inch screens that can be managed using Panasonic COMPASS.

For more information visit
business.panasonic.co.uk/computer-product/COMPASS

Panasonic
BUSINESS

For more information please visit:

business.panasonic.co.uk/computer-product/COMPASS

Computer Product Solutions (CPS) BU, Panasonic System Communications Company Europe (PSCEU), Panasonic Marketing Europe GmbH, Hagenauer Straße 43, D-65203 Wiesbaden (Germany).

TOUGHBOOK TOUGHPAD

1_00114934_SEPT 2016_EN_V4