Mobile operating systems are changing - Are you ready?

Operating systems used within rugged mobile devices have evolved greatly over recent years, and these changes bring with them both challenges and new opportunities for operators.

Ten years ago, operating systems for mobile devices were provided by Microsoft. Windows CE and Windows Pocket PC (latterly Windows Mobile and Windows Embedded Handheld) offered features and capabilities needed for deployment in rugged supply chain environments. At that time, Apple had only recently launched the first iPhone and Google had acquired Android, but was yet to bring a new device to market. Outside of these players, other options available were largely focused around the white collar professional user and proved largely unsuitable for the unique needs of a rugged device.

Today, things have changed, with Microsoft retreating from the enterprise mobility environment. Organisations currently running applications that require a legacy Microsoft mobile operating system (Windows CE 6 or Windows Mobile/Windows Embedded Handheld 6.5) will soon face the end of support for their platform. Mainstream support, which includes regular updates, has ended for both legacy systems. Microsoft extended support (security fixes etc.) will end for Windows CE 6 this year and for Windows Embedded Handheld 6.5 at the beginning of 2020.

After those dates, organisations will be unable to obtain fixes should a vulnerability or error be found in Microsoft code. As a result, many organisations are already transitioning to new applications running under alternative operating systems, yet others are left wondering where to turn.

Preparing for tomorrow, today

As end of support dates for legacy Microsoft operating systems approach, organisations need to make plans to move forward, as mobile application development can require considerable time and effort. One way to provide more time to make decisions is to select hardware that can support multiple operating systems.

Manufacturers such as Zebra Technologies and Honeywell are already offering rugged mobile devices, running Windows CE 7 or Windows Embedded Handheld 6.5 that can be converted to Android at a future date. This allows existing legacy applications to continue running until the organisation is ready to move to Android, at which time a small investment in a software conversion is required; no changes are required to the hardware.

Android has evolved and enhanced its security

Given the negative impacts that data breaches can have on businesses in the digital age, organisations have relied on Windows operating systems due to its strong security model. This model sought to promote system stability and went much further than the security functions available on any other operating system at the time.

Using Android allows companies to access a large ecosystem of applications, development tools and resources, but also previously involved security risks that needed to be addressed and mitigated. Android, though, has steadily evolved its approach to security over recent years. As its market share has grown, Android has become a target for exploits and malware attacks. Google has responded by increasing the protections to prevent the introduction of Potentially Harmful Apps (PHA), as well as implementing defences inside the operating system that limit the ability of the system to be compromised. Today, Android is a much more secure operating system, utilising application isolation and encryption enabled by default to protect personal and corporate data, as well as exploit mitigation techniques to provide a high level of security to the user.

Added security through advanced devices

To help manage the transition to Android and alternatives to Windows, as well as offer an extra layer of device security, advanced enterprise mobile device manufacturers have their own cybersecurity teams in place. These teams monitor multiple information sources to learn of potential security issues as early as possible (typically well before the mainstream media) and have implemented an escalation protocol that mobilises resources company-wide on a priority basis to address these issues. Once an Android vulnerability is revealed and a corrective action posted by Google, security experts implement the fix and deliver it to customers. Direct distribution of patches and updates enables device manufacturers to reduce response time, protecting valuable data.

Many enterprise customers will choose to restrict end-users by 'locking down' the device through the use of a mobile device management (MDM) product or an app provided by their device manufacturer. These tools control user access to system resources and can restrict the system to execute only designated apps. Removing the user's ability to install or run unauthorised apps makes the system far less vulnerable to security exploits caused by user actions. Businesses can establish application white lists or blacklists, control the availability of a wide range of device features, and control which IP addresses are accessible through the firewall. By limiting what the user can do with the device, IT support becomes easier and opportunities for the introduction of malware into the system are substantially reduced.

Android is the safe choice, but is it enterprise-ready?

Most of us know Android. It's in our phones, Chromebooks, cars and TVs. As Google says, it's 'the world's most popular mobile OS'. Over the past few years, we've seen Android move strongly into more use cases in the enterprise arena. Its familiar user experience and trusted performance makes it a popular choice, but it still poses a few challenges for enterprise, especially across e-commerce fulfilment, warehousing, transport and logistics. The key issue springs from Android's roots as an operating system for consumer devices. The frequency with which new versions are released (almost every 12 months), and the support life-cycle for each version of Android (generally 3 years, after which security support stops) is fine for consumers who are used to upgrading to a new phone or device regularly, but businesses typically expect at least a five year service life from a technology investment. So, businesses could again be facing the dilemma of using devices that don't have security support and leaving themselves exposed to risks, or swallowing the extra cost and inconvenience of migrating to a new OS more frequently. Neither of which is satisfactory.

Zebra & Honeywell understand this dilemma, and have developed software security solutions that extend the lifespan of Android devices and close the security gap. To help address these issues, Zebra has introduced LifeGuard for Android, and Honeywell has developed the Mobility Edge Platform, both of which reduce the cost and time to deploy, manage, optimise and secure Android mobile devices. Platforms such as these are particularly useful for organisations that scale their operations with seasonal workers and need to cover any skills gap through simplified user experiences. While there is no substitute for a well-skilled workforce, applying advanced technological tools with the right operating system support gives organisations unparalleled levels of operational control.

Preparing for a pain-free transition

Transitioning from legacy Windows platforms to Android involves writing new apps, adapting workflows and changing the mobile devices that workers use, which can prove to be a significant undertaking for any IT department.

To find out how OpalTec can help your organisation transition from a Windows based operating system to Android, please call OpalTec's Solutions Specialist James Mellor on 0117 916 0810 or send him an email jgm@opaltechnology.com