Honeywell

THE POWER OF **CONNECTED**

MOBILE OPERATING SYSTEM TRANSITION

Insights and Considerations

Introduction

A shift in the mobile operating system landscape has occurred over the last several years. The transition from legacy Windows® is well underway. While there remain several distinct choices on the roadmap, the tradeoffs and compromises associated with each have become clearer. This paper will elaborate on these points and provide the reader with guidance on recommended solutions.

Barcom, Inc.
4136B Jersey Pike
Chattanooga, TN 37421
423-855-1822
www.barcominc.com

Table of contents

3 Mobile Operating System History

4 Legacy Operating Systems

5 Android Enterprise Evolution

6 How Honeywell Helps

8 Android Lifecycle Management

10 Conclusion and Recommendations

Mobile Operating System History

For the open source Android operating system, Google OEMs and third parties began developing extensions that enabled device management capabilities, provided more control over user actions, and added support for industrial Wi-Fi networks and barcode scanning capabilities.

Ten years ago, operating systems for mobile devices in the enterprise space were provided by Microsoft. Windows CE and Windows Mobile (later Windows Embedded Handheld) offered features and capabilities needed for enterprise deployment, while a robust ecosystem of developer tools and third-party offerings allowed customers to create the solution needed to effectively operate and manage their businesses. Apple had only recently shown the first iPhone®. Google acquired Android™ a few years earlier and had yet to see a phone come to market. Other options available at that time were largely focused around the white collar professional user and proved largely unsuitable for the unique needs of the purpose-built enterprise environment. Windows proved to be a solid choice and was selected by the vast majority of customers deploying rugged mobile devices for line-of-business applications.

The emergence of enterprise features in iOS and Android did not occur until several years later and initially evolved rather slowly while Apple and Google focused on the rapidly growing consumer phone market. For the open source Android operating system, Google OEMs and third parties began developing extensions that enabled device management capabilities, provided more control over user actions, and added support for industrial Wi-Fi networks and barcode scanning capabilities. This enabled the first round of Android devices targeted at enterprise deployments, gave rise to several rounds of improvements, and broadened product offerings as customers reacted positively to user-friendly touch interfaces and a growing ecosystem of apps and developers. However, this entrepreneurial approach also gave rise to fragmentation. As the level of modification to the base operating system increased, the further it diverged from the standard, making it harder for applications to run across different vendors' products and much less likely that highly modified devices would progress quickly to the next version of the base operating system.

Apple responded with its own management tools and enterprise enhancements to iOS, and has a large developer ecosystem. However, Apple's closed system continues to have limitations in terms of controlling updates and managing some device features. Since hardware devices are limited to consumer phones and tablets, iOS is a viable solution for use cases that demand a mobile device that is only ruggedized via the addition of external caseworks.

Legacy Operating Systems

As end of support dates for legacy operating systems approach, customers need to make decisions and plans to move forward, as application development can require considerable time and effort.

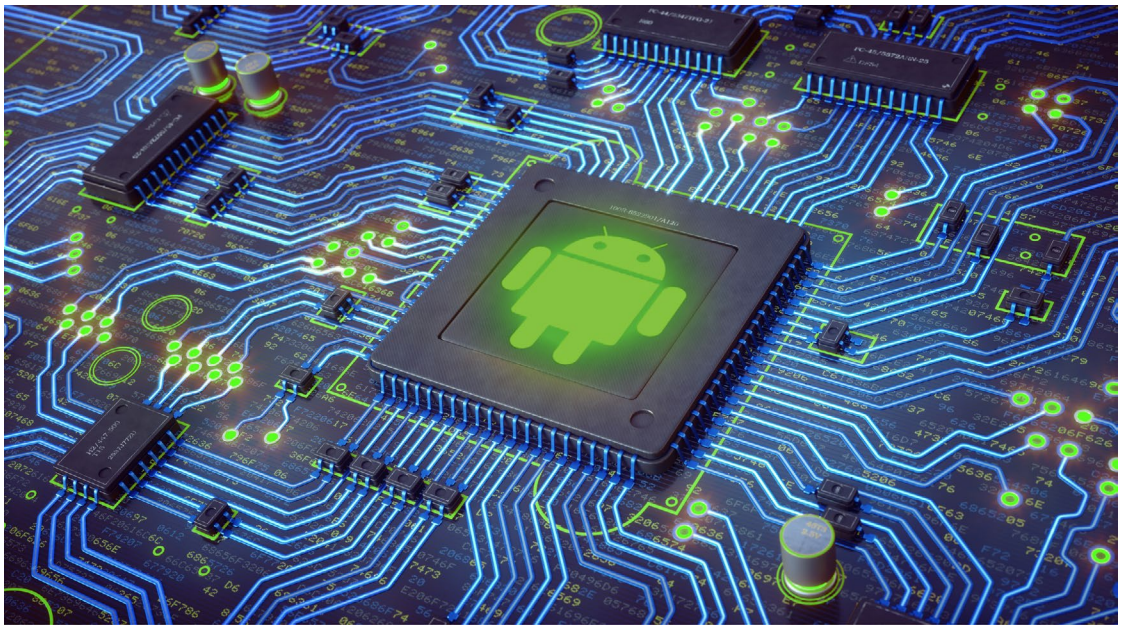
Customers currently running applications that require a legacy Microsoft operating system (Windows CE 6 or Windows Mobile/Windows Embedded Handheld 6.5) will soon face the end of support for their platform. Mainstream support, which includes regular updates, has ended for both legacy systems. Microsoft extended support (security fixes) will end for Windows CE 6 in early 2018 and for Windows Embedded Handheld 6.5 in early 2020. After those dates, vendors will be unable to provide patches should a vulnerability or error be found in Microsoft code. For this and other reasons, many customers have begun planning a transition to new applications running under a modern operating system.

As end of support dates for legacy operating systems approach, customers need to make decisions and plans to move forward, as application development can require considerable time and effort. One way to provide more time to make decisions is to select a hardware offering that can support multiple operating systems. The Honeywell CN75 and CK75 Series mobile computers, along with the Honeywell CN51 mobile computer, offer a choice of Windows Embedded Handheld or Android. In addition, customers purchasing Windows Embedded Handheld can convert their devices to Android at a future date. This allows existing legacy applications to continue running until the organization is ready to move to Android, at which time a simple field-based software conversion is performed. Only a small investment in software is required; no changes are required to the hardware.

Android's large market presence supports a broad variety of OEMs and hardware form factors, making it more likely that a device is available to meet the customer's use case and cost requirements, including devices that offer integrated physical keypads.

Android Enterprise Evolution

Google has continued investing heavily in enterprise capabilities in each of its last three versions, renaming Android for Work to Android Enterprise.



Prior to 4.0 Ice Cream Sandwich, Android offered little in the way of enterprise features. The consumer-focused operating system was augmented by OEM extensions and third-party software to allow it to be controlled and managed in the enterprise environment. Enterprise features gradually began appearing in 4.2 Jelly Bean and 4.4 KitKat releases, culminating with the introduction of Android for Work in 5.0 Lollipop. Android for Work provided an extended set of management APIs and a container system for separating and independently managing personal and work apps and data.

Google has continued investing heavily in enterprise capabilities in each of its last three versions, renaming Android for Work to Android Enterprise. Added features include bulk provisioning to speed device setup, Device Owner mode to allow fully managed devices at the corporate level, always-on VPN, and encryption enabled by default to protect personal and corporate data.

Popular mobile operating systems such as Android enable companies to access a large ecosystem of applications, development tools, and resources, but also involve security risks that must be addressed and mitigated. Android has steadily evolved its approach to security.

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 (PHAs), as well as implement defenses inside the OS that limit the ability of the system to be compromised should a PHA be installed. A few of those protections are discussed below. Detailed information is available in Google's Android Security 2016 Year in Review report located here:

https://source.android.com/security/reports/Google_Android_Security_2016_Report_Final.pdf

How Honeywell Helps

The cybersecurity team monitors multiple information sources to learn of potential system security issues as early as possible (typically well before the mainstream media) and has implemented an escalation protocol that mobilizes resources company-wide on a priority basis to address these issues.

Honeywell is strongly committed to cybersecurity. Our global businesses include aerospace and process solutions that demand a very high degree of security in all aspects of operations. A corporate-level cybersecurity task force sets and maintains security policies and standards, including test procedures used during product development that specifically identify software issues that could make systems more vulnerable to exploits. This approach eliminates potential vulnerabilities before products are even released.

The cybersecurity team monitors multiple information sources to learn of potential system security issues as early as possible (typically well before the mainstream media) and has implemented an escalation protocol that mobilizes resources company-wide on a priority basis to address these issues. Once an Android vulnerability is revealed and a corrective action posted by Google, Honeywell's Android security experts implement the fix and deliver it to customers. Direct distribution of patches and updates enables Honeywell to reduce response time compared to OEMs who must go through secondary channels to deliver their updates.

Security Manuals are published for all Honeywell products to guide customers in implementing best practices to secure their environment and devices. Guidance is provided in configuration of device settings, network settings, and maintaining a secure IT environment. These preventative measures are intended to reduce the avenues through which threats can enter the customer environment.

Many enterprise customers will choose to restrict end users further by "locking down" the device through the use of a Mobile Device Management (MDM) agent or an app such as Honeywell Enterprise Launcher. 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 unauthorized apps makes the system far less vulnerable to security exploits caused by user actions. Honeywell offers an Enterprise Toolkit API Library that enables customers to establish application white lists or black lists, control availability of a wide range of device features, and control which IP addresses are accessible through the firewall. Honeywell Launcher replaces the standard Android home

screen with a kiosk experience that allows the user to see and execute only the apps needed to perform their job. Honeywell also offers an Enterprise Browser that enables web page rendering using standard Android controls, but controls the sites that users are allowed to access. 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.

Another important aspect of security is maintaining an updated system. Researchers are constantly discovering and responsibly reporting vulnerabilities in the Android code base that could potentially be subject to malicious exploits. Google even offers a bounty program to encourage researchers to find and report potential issues. Google and chipset providers such as Qualcomm provide security patches to OEMs on a regular basis for incorporation into their software builds. Honeywell updates their Android system images on a regular 60-day cadence, with patches for extremely critical exploits available within just a few days (as necessary). Patches are delivered as incremental updates to baseline images, minimizing the size of the update package for easier deployment across the customer's network. Unlike consumer OEMs, Honeywell packages are downloadable from a web portal to allow for customer acceptance testing prior to full-scale deployment. An email notification subscription is available so customers will be informed as soon as new updates are posted.

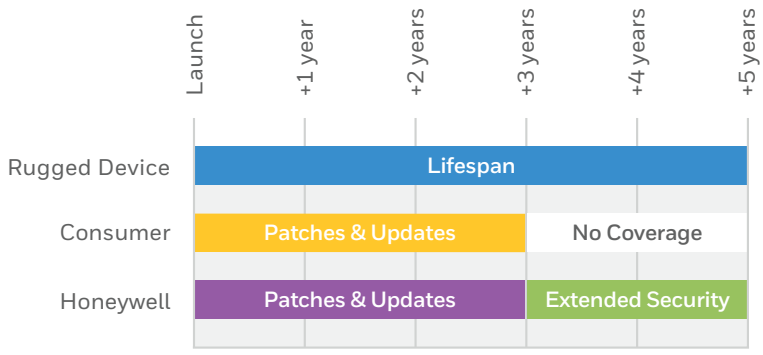
Android Lifecycle Management

Honeywell offers a program to provide patches for severe security vulnerabilities applicable to the supported operating system on a periodic basis for 2+ years after Google security patch support ends.

Customers deploying mobile computer solutions in the rugged enterprise environment expect a longer usage cycle than consumers. Where smartphones in consumer use cases generally turn over in 2–3 years, enterprises are expecting their systems to last 3–5 years or longer. Historically, embedded operating systems used in rugged mobile computers had a lifecycle corresponding to enterprise use cases. Windows CE and Windows Embedded Handheld are being supported by Microsoft for 10 years after initial introduction.

Although Android has been augmented by Google with a variety of new enterprise features with each major release, extended support is not among them. Android major versions (or "dessert releases") occur on a roughly annual basis and are generally supported with security patches from Google and chipset vendors for a period of 3 years thereafter. This creates a gap in support coverage relative to enterprise expectations. Selecting OEM chipsets that are supported for subsequent dessert releases will help extend the timeline, but ultimately Google support policy stops short of enterprise customer expectations.

Honeywell offers a program to provide patches for severe security vulnerabilities applicable to the supported operating system on a periodic basis for 2+ years after Google security patch support ends.



- Timing of delivery to customers will be quarterly, or less if no severe patches applicable to the supported operating system version are reported. Applicable patches will generally be delivered within 90 days of public disclosure with exceptions possible for imminent threats.
- Customers utilizing this service will be expected to apply all previously released patches in order to apply the most recent patch. In other words, patches are cumulative relative to the last OS maintenance release. Specific patches cannot be applied individually.
- Security patches will be tested following Honeywell standard test procedures applicable to all software releases. It remains the responsibility of the customer to test any software updates received from Honeywell to their satisfaction prior to rolling out an update to their estate.
- Customers would receive these benefits under the terms of a service contract, either standalone or incorporated into another type of service agreement. Customers without a contract would not receive security patches after Google security patch support ends.

This program will be available on Honeywell devices running Android 6.0 Marshmallow and later versions, upon expiration of Google security patch support.

Conclusion and Recommendations

Android is a secure operating system, utilizing application isolation and exploit mitigation techniques to provide a high level of security to the user. Implementing lockdown techniques via an MDM or Honeywell Enterprise Launcher can further reduce the risk of malware intrusion by limiting what the user can do and what apps can run on the system.

Honeywell's products are designed from the start to meet Honeywell's rigorous security standards. Security is evaluated throughout the development process, identifying and mitigating vulnerabilities even before products are released. Education of customers and constant monitoring of security vulnerabilities and exploits, with defined processes for addressing those issues that are discovered, further protect our customers' systems from compromise. A subscription-based notification model enables customers to take immediate action to mitigate risk while software is being patched and tested. Customers can be assured that their systems are designed and supported to the highest standards and they can operate their businesses with confidence knowing Honeywell is working to help them maintain the security of these systems.

Honeywell offers solutions for all three major operating systems in the rugged mobile enterprise space: Android, iOS, and Windows. For several years, Honeywell has maintained a neutral stance with regard to operating system choice on mobile computers, encouraging customers to consider many factors to determine the best operating system choice for their particular environment.

With its large market share and extensive ecosystem of apps, developers, and VARs, Android has become the clear choice for many enterprises in a variety of industries. Transitioning to Android involves writing new apps, adapting some workflows, and changing the mobile devices workers use. This can be a lot to do at once. One way to provide more time to make decisions is to select a hardware offering that can support multiple operating systems. The Honeywell CN75 and CK75 Series mobile computers, along with the Honeywell CN51 mobile computer, offer a choice of Windows Embedded Handheld or Android. In addition, customers purchasing Windows Embedded Handheld can convert their devices to Android at a future date. This allows existing legacy applications to continue running until the organization is ready to move to Android.

Barcom, Inc.
4136B Jersey Pike
Chattanooga, TN 37421
423-855-1822
www.barcominc.com

Mobile Operating System Transition – Insights and Considerations | Rev A | 10/17

Honeywell