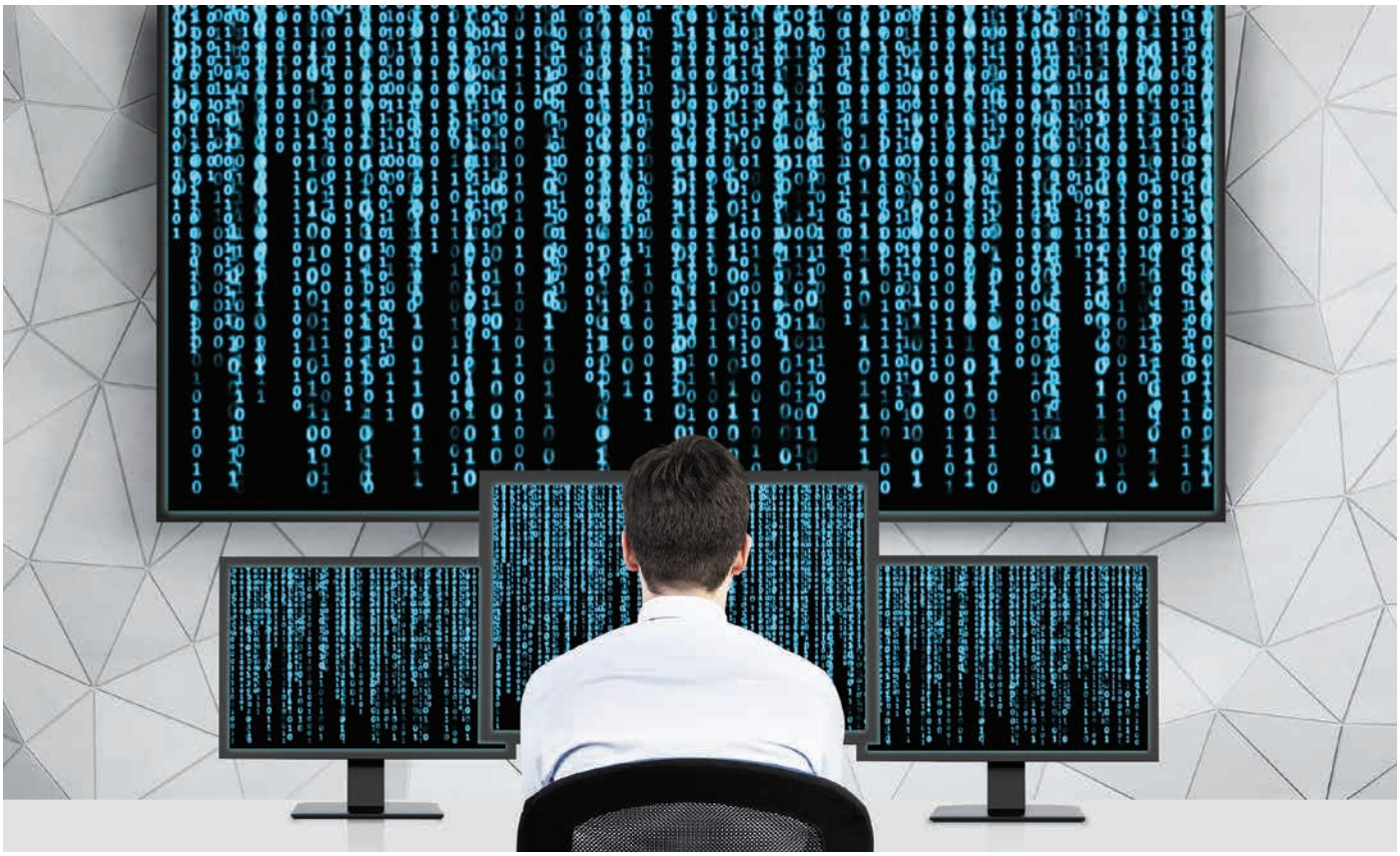
VISIONiD

Empowering Enterprise Intelligence

WHITE PAPER

KEY CONSIDERATIONS WHEN CHOOSING A MODERN MOBILE OPERATING SYSTEM



Key Considerations When Choosing a Modern Mobile Operating System

When migrating to a new mobile operating system, organisations should carefully consider essential components required to deliver long-term operational success.

The Workforce Mobility Revolution is upon us and with it brings a tremendous opportunity for organisations to increase their operational efficiencies and productivity while at the same time save money. New technologies and consumer-friendly hardware and software running on enterprise-class platforms are making it easier than ever to deploy a successful field mobile strategy. Many organisations are already using modern rugged handheld devices and plenty more are ready to integrate them into their workflows.

While mobility is on the rise, a major shift is occurring in the mobile operating system (OS) landscape. Devices that have been deployed for over a decade are reaching end-of-life and new options are emerging. As Microsoft prepares to end support for existing Windows mobile OS devices in 2020, other players have made in-roads. Google has transformed its Android OS into an enterprise-ready platform with a user interface that mirrors that of consumer-grade devices making adoption infinitely easier.

Choosing a new mobile OS is just the beginning. Before making a decision, organisations should consider requirements from the IT department, mobile workforce and developers. Applications may need to be rewritten, data transferred and new devices provisioned. New technologies such as beacons, sensors, Near Field Communication (NFC) and GPS bring new functionalities that can give organisations a competitive edge. Security also plays a critical role, and there are many facets to examine: the device, safeguarding data, company protocols and industry requirements.

This paper explains what each platform offers along with the features and technologies available to help you make an informed decision when choosing a mobile OS. Whether you are just getting into the mobile space or dealing with devices that are reaching end-of-life, this white paper provides an overview of key features and considerations to keep in mind as you consider which OS is right for your organisation.

Current State of the OS Market

Historically, Windows has been the leading choice for mobile devices in the workforce. Microsoft's Windows Mobile and Windows CE platforms were developed specifically for the enterprise market and have served their purpose extraordinarily well.

When enterprise-grade mobile devices first emerged, organisations had already invested in a Microsoft infrastructure. Naturally, when it came to selecting a mobile operating system they needed one that would work seamlessly across multiple platforms and Microsoft OS was the only option.

Much has changed since then. Today, consumer-centric mobile devices have made their way into the enterprise and organisations have begun modifying their infrastructure to support them. As new ways to use mobility in the workplace were identified, it opened up a wide variety of applications and challenges. The result is clear: consumer operating system adoption is essential to a successful mobile solution in the enterprise. Without it, economies of scale cannot be achieved.

THE FUTURE OF WINDOWS MOBILE

As new consumer OSs are finding a home in the enterprise space and Windows 10 is on the horizon, Microsoft has ended mainstream support for its legacy operating systems.

What does this mean? Among other things, the end of mainstream support means no new security protocols. Microsoft will continue extended support and provide security patches for Windows Embedded Handheld (WEH) 6.5 until the beginning of 2020.

Similarly, Microsoft will provide Windows CE 6.0 with extended support through the end of Q1 2017 and Windows Embedded Compact (WEC) 7 will be supported until Q1 2021. In addition to minimal support and diminishing security, it's also a signal that no new devices will emerge and many existing models are approaching end-of-life.

The next generation of Windows 10 IoT Mobile Enterprise is on the horizon. Along with its highly anticipated new features, comes an exciting new architecture. The new Microsoft architecture is vastly different than that found on legacy platforms. The good news is that you will be able to bring your existing mobile applications along, but they will have to be rewritten to support the new architecture and you will need to re-architect applications to run on forthcoming Microsoft-enabled mobile devices.

Couple the need for consumer adoption with the lack of updates and limited support for Windows Mobile and Windows CE and one thing is certain: Legacy Microsoft mobile devices have a very short lifespan. So what are the mobile OS options going forward?

Microsoft Windows CE 6.0
Extended support through the end of Q1 2017

Windows Embedded Handheld (WEH) 6.5
Extended support and security patches until the beginning of 2020

Windows Embedded Compact (WEC) 7
Supported until Q1 2021

Legacy Microsoft mobile devices have a very short lifespan. So what are the mobile OS options going forward?

The Android Opportunity

83%

Google Android OS global consumer market share

74

Enterprise Android devices available from 22 manufacturers

Google Android OS is gaining ground with IDC reporting the OS has 83% of the global consumer market share. Currently, there are over 74 enterprise Android devices available from 22 manufacturers and that includes an additional 40 products that have come to market within the past year. There's good reason for its success: it's open, flexible, compatible with Microsoft and it offers the kind of control IT demands.

The Android architecture is similar to the previous Microsoft Windows Mobile OS. Android can work within an existing Microsoft infrastructure. The platform supports popular Microsoft products such as Workplace Join, Intune, Outlook, Azure Mobile Services, Office and Office 365, OneDrive, and Cortana. It can sync Google applications and Outlook. In fact, developers can create Android applications in Visual Studio.

There are four essential flavors of Android OS to consider. The fact that there are so many options shows that it's flexible enough to customise the OS to meet your specific needs with the level of security required to safeguard your enterprise data and devices.

Google Mobile Services (GMS). GMS is a consumer-centric solution. It's comprised of a set of popular Google applications and cloud-based services that are available through a license with Google. You can install corporate applications on the devices. GMS includes access to the Google Play Store and other services where data is shared back and forth with Google. This makes GMS potentially vulnerable to security issues. So if you're looking for a solution where you ultimately control the device, the GMS option may not be the right fit for your organisation.

Android Open Source Project (AOSP). AOSP is a slimmed down version of Android and can be customised for specific device requirements. It's still the Android OS, but it doesn't have Google services that require the device to call Google or provide location information.

Android for Work. Recently introduced by Google, Android for Work incorporates aspects from both Google Mobile Services and AOSP. It incorporates Google Play for Work, which is essentially an enterprise app store. With Google Play, organisations can access a private app store and decide which applications are approved for use on their devices. With Android for Work, you can:

- Push applications to devices from the store
- Choose if the application resides in the cloud or on the device
- Handle bulk application provisioning and licensing
- Gather user ratings and feedback

Since Android for Work is part of Google Mobile Services, data is shared back and forth with Google which may pose security concerns to astute IT professionals.

Android for Work provides managed profiles, a feature also found in AOSP. With this feature, users can carry one device with two separate profiles: one for work and one for personal use. Applications have a badge signifying work or personal. The data used is entirely independent for each profile. Android for Work is geared specifically for organisations that allow employees to use their personal device for work.

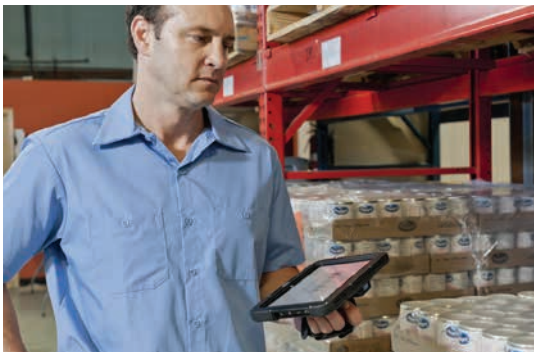
Android for Work also offers a second managed profile option called Corporately Owned Single User (COSU). COSU is ideally suited for kiosks and rugged field devices that make use of a single managed profile with full administrator control.

Zebra's Android with Mx. The Mx solution fortifies the Android operating system with a layer of features that infuses standard Android (either AOSP or GMS) with the characteristics required to take full advantage of Android devices in your organisation.

With Android as its foundation, Zebra Mx adds a layer of security, mobile application management and device management features that are essential for enterprise-grade mobile computers and devices. Mx enables enterprise-class security and business-class Wi-Fi connectivity, which are crucial for voice applications.

With Mx on AOSP, you are in complete control of your mobile computers and devices. You decide which applications get installed and when to push updates. You decide if and when to activate features. With Mx on GMS, the above is mostly still true, but there may be some GMS features (like the play store app) that update directly from Google.

Mx is not a proprietary version of Android. Furthermore, it does not reduce any Android functionality or create application compatibility issues. Mx is customised to fit your needs and is fully compatible with standard Android applications. Mx does not require any licensing fees.



LIMITATIONS OF APPLE IOS

Apple iOS is also an option for the enterprise environment, but adoption is slow. What makes iOS devices appealing to consumers, namely stylish design and its closed system, are deterrents in the enterprise market. Devices found in the enterprise must be tough enough to withstand rigorous usage and a myriad of environmental conditions. Features typically not associated with Apple's sleek, consumer design.

With the iOS' closed system, software updates, security patches, applications and user access, to name just a few, are controlled by Apple. When you use an Apple device your data is being mined, which can be unsettling and may pose a potential security risk to your data and devices.

Apple iOS also makes it extremely difficult for IT to remotely manage your devices, including the ability to lock down settings, remotely stage updates, troubleshoot, lock, wipe and monitor devices. This vulnerability can lead to potential device issues, increased employee downtime and IT overhead.

Key OS Considerations

When it comes to picking a mobile OS, it shouldn't be done in a silo. Many parts of your organisation will be affected by your choice. It's important to consider the needs of IT, finance, and those who will actually be using the devices in the field before making a decision.

In addition to compiling a list of must-have features, also identify the issues employees currently encounter. Understanding both the pros and cons of an existing solution will help prioritise your overall feature list. This list of features will help guide the decision-making process whether you're just getting started with a mobile OS or considering switching to a different option.

If you choose an OS that's closed such as iOS, Windows 10, or Google Mobile Services, the data gets mined by Apple, Microsoft and Google respectively making it potentially vulnerable

SECURITY

Security involves a multitude of features and should be a top priority for any organisation considering its OS direction. It goes beyond securing the device and safeguarding data. Here is a high-level breakdown of security considerations:

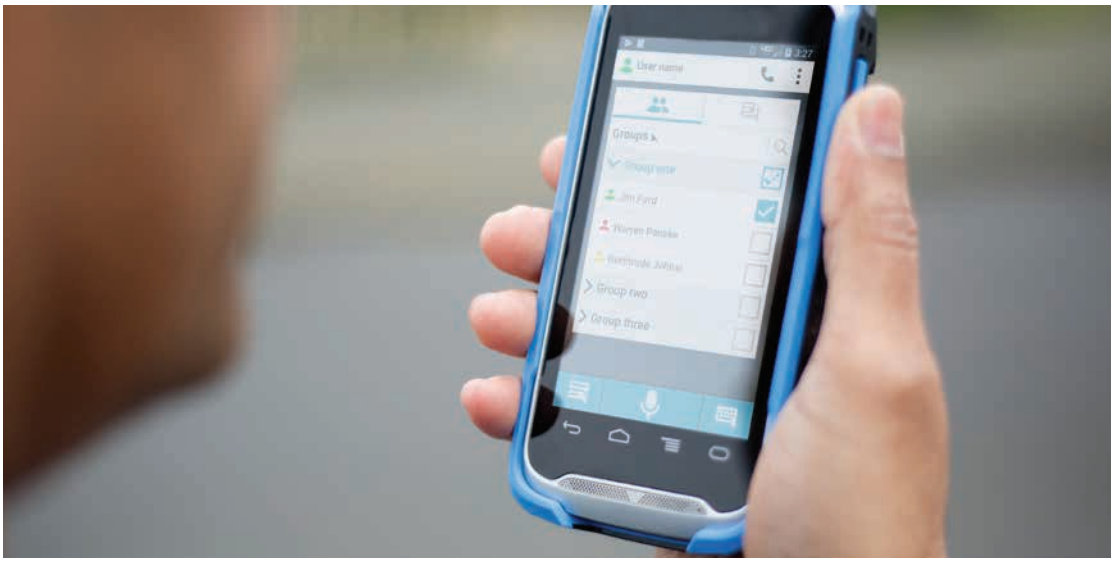
Data Protection: Consider how data is protected whether it resides internally or in the cloud. Virtual Private Networks (VPNs) are useful when data travels on untrusted/ public networks. Also, think about where that data goes. If you choose an OS that's closed such as iOS, Windows 10, or Google Mobile Services, the data gets mined by Apple, Microsoft and Google respectively making it potentially vulnerable.

Device Protection: When devices aren't locked down, users can inadvertently install malware by visiting unsecure websites and downloading unauthorised applications. When administrators control the user settings and enable access to only authorised features, the device and its data are inherently safer. It's also important to consider what happens to devices if unauthorised personnel access them. Features like password protection and locking down a device after a period of inactivity on the network are essential.

Mobile Device Management (MDM): Administered by an MDM vendor, this is how administrators control and manage the device. It's what is used to get applications on the device. Each OS has unique approaches to interacting with an MDM. Enhancements can include locking user settings so changes can't be made, using exchange active sync policies, and pushing a digitally signed XML configuration to a device.

Enable and Facilitate Regulatory Compliance: Verticals such as retail, healthcare, and government have unique security requirements separate from what's on a device. For example, the Payment Card Industry Data Security (PCI-DSS) defines a comprehensive solution for securing payment transactions. In general, any company that accepts debit or credit card payments is required to comply. Look for a mobile OS that provides a way for you to easily meet those requirements and install security patches now and in the future.

Secure and Managed Wi-Fi Connections: Consumer-centric devices are typically designed to work with household or corporate Wi-Fi networks. In the field, a device can easily roam to multiple Wi-Fi access points. Besides being unsecure, users can also encounter lag time as they move between access points. This is unacceptable for those who need to enable voice applications. A few seconds of delay in a voice app means part of the conversation is lost, which isn't a good user experience.



APP PROCUREMENT AND OS UPDATES

How do you get applications on the device? Does your IT team want to rely on the user downloading the app or would they rather push the application out? If you opt for allowing users to download applications themselves, it could be accomplished through a public app store such as Apple's App Store or Google's Play Store or through a private, corporate app store where you control which applications are available.

In closed systems, the OS creator controls (for example, Apple) how and when to push updates out to devices. As such, users are forced to install the update. While you may be able to hold off on installing the update in some instances, eventually the OS will no longer be supported. This can cause a lot of issues. After all, updates can often be buggy resulting in reduced user productivity and increased calls to IT for support. Secondly, you may not want to install the updates. Many devices in the field often run on the same version of an OS for years without issue. If you're using Android AOSP, updates to the OS are at your discretion and on your timetable.

WEB-BASED APPLICATIONS

More and more organisations are using web-based applications since they run on multiple platforms. Issues can arise when a web browser is required to access the app, which can potentially create security risks. To avoid this, pick a solution that has a browser that you can control and manage. For example, operating systems that are closed such as iOS may not offer a way to control the web experience.

LICENSING FEES

Microsoft traditionally requires per-seat licensing fees for many of its products. If you're deploying a lot of devices, this can quickly become expensive. It also adds another level of maintenance when it comes to ensuring that the licenses are current. If you opt for an OS that requires a licensing fee, consider a device provider that includes that cost in the total cost of ownership (TCO).

PROVISIONING DEVICES

Setting up devices can be extremely taxing on administrators especially when a large number of units have identical configurations. Instead of setting up each device individually, ensure that the OS you select supports Mobile Device Management (MDM) tools that help you effectively stage multiple devices at one time.

If you're using Android AOSP, updates to the OS are at your discretion and on your timetable

32%

Over the past couple of years Android devices have gained adoption in the industrial handheld market and represent 32% of the market

SUSTAINING COSTS

How much does it cost to maintain the OS for the life of the device? This includes handling updates, deploying patches and support. Evaluate the type of support available even after an OS reaches its end of life.

USER-FRIENDLY/ TRAINING REQUIRED

One of the main benefits of going with a mainstream mobile OS is that users are already familiar with the interface. Legacy Windows Mobile devices that have been in the field for over 10 years offer a different user experience than that of today's consumer devices. The UI is not intuitive and requires much more training. Whereas, if you have a solution that's similar to what is already being used by workers in their daily personal lives, the learning curve will be greatly reduced.

CUSTOMISABLE

This takes into account features such as specifying user settings, deciding what's accessed on the device and when to install updates. However, it also includes managing CPU processes in the background. For example, you may want a voice app running in the background. In a closed system, this might not be efficient because it will drain the CPU and battery life.

CHOICE OF DEVICES

One sign that a mobile OS has longevity is the number of devices running it. Windows 10 is still on the horizon, so we can't say how many devices will be available. Over the past couple of years Android devices have gained adoption in the industrial handheld market and represent 32% of the market.

SELECTING A MODERN OS

Whether you're just entering the enterprise mobile space or are contemplating making the move to a new OS, the best thing you can do is be informed. Be sure to weigh the pros and cons of every mobile OS you're evaluating including IT needs, device availability, user friendliness and TCO. We know choosing a mobile OS is a serious commitment and are dedicated to giving you the right tools and information to help you understand the current landscape, available options and key considerations.

Lower your IT administrative costs

Get better performing, intuitive applications

Provide a superior user experience (UI, device performance)

How VisionID Can Help

For the Android OS, VisionID offers a suite of software solutions that help you customise and control the experience. At the heart of our Android offering is Mobility DNA, a simplified end-to-end solution that includes enterprise applications, administration utilities and development tools. It provides everything you need to get Android devices up and running in the enterprise with the security you require.

Android with Mx: A suite of extensions that comes installed on all Zebra Mx Android devices. At the base of the system is Android AOSP. Android GMS versions are also available for most devices. Our extensions provide enterprise-class security, business-class Wi-Fi connectivity, and the ability to manage application installations, OS updates, and patches.

StageNow: A tool to provision Android devices either through a barcode or NFC quickly. The first device is provisioned and a barcode containing all of the device settings is printed. Each new device scans the barcode, and the network settings and provisioning information are used to automatically configure all devices that need those settings.

Enterprise Mobility Development Kit (EMDK): With a comprehensive set of APIs and sample code, you can quickly take full advantage of the purpose-built capabilities our devices have to offer (such as barcode scanning and profile management) in your Android application.

Enterprise Browser: An OS agnostic mobile application development tool that allows developers to seamlessly integrate the native peripherals of a device into web based applications, while enabling barcode scanning, signature capture and much more.

App Gallery: Create a corporate app store on your devices. In addition to your applications, you can populate it with approved third-party applications.

Wide Selection of Devices: VisionID offers over 12 different Android models and supports the Texas Instrument, Qualcomm, and Intel processor platforms. Since it's the Android platform that consumers are already using, the devices are easy to deploy and require minimal training. On the Microsoft front, we continue to offer many of the existing models and support legacy units that are in the field. We are working closely with Microsoft on Windows 10 and will offer options when it becomes available.

VISIONID
Empowering Enterprise Intelligence

Head Office: Unit 4C Gurtnafleur Business Park, Clonmel, Co. Tipperary, Ireland
Telephone: +353 (0)52 618 1858 Facsimile: +353(0)52 618 1860 Email: info@visionid.ie

Limerick Office: Roselawn House Office Services, University Business Complex, National Technology Park
Telephone: +353 (0)61 514 683 Facsimile:+353 (0)61 749 873 Email: midwest@visionid.ie

Dublin Office: 3013 Lake Drive, Citywest Business Campus, Dublin 24, Ireland
Telephone: +353 (0)1 524 1586 Facsimile: +353 (0)1 443 0560 Email: dublin@visionid.ie

North. Ireland Office: 20 Adelaide St. Belfast, BT2 8GB, Northern Ireland
Telephone: +44 (0)28 9099 8504 Email: ni@visionid.co.uk