BALANCE BETWEEN EMBEDDED OPERATING SYSTEM SECURITY FEATURES AND ADDITIONAL HARDWARE/ SOFTWARE BASED PROTECTION NEEDS CAREFUL CONSIDERATION

Organisations in Australia, the UK and the US can Benefit from Android Security Features Which Extend Beyond Native Operating System Capabilities

Survey conducted by IDG Connect on behalf of Samsung

Role:
Organisation Size:
Region:
Buying Stage:

IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilises access to 38 million business decision makers' details to unite technology marketers with relevant targets from 137 countries around the world. Committed to engaging a disparate global IT audience with truly localised messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide.

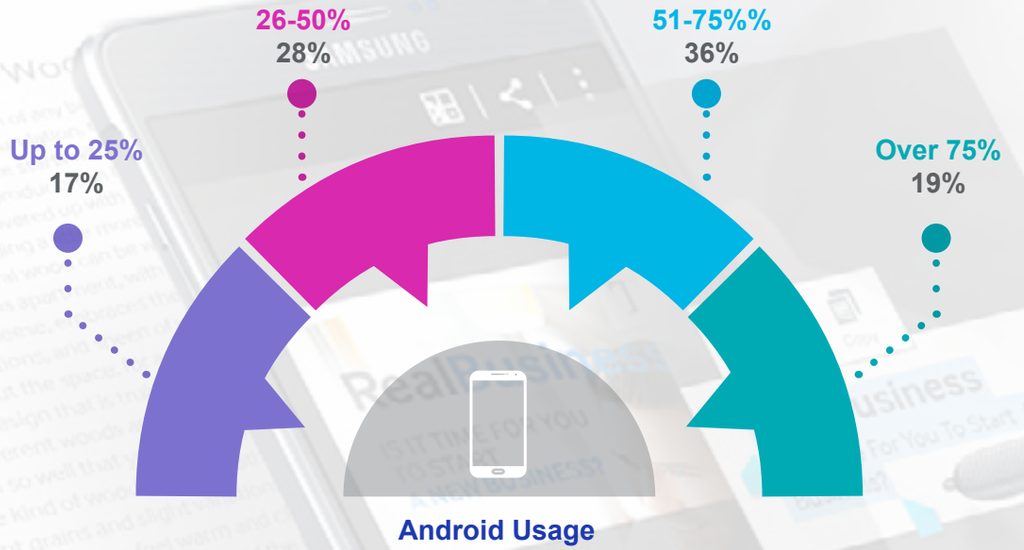
Summary of Research

Ability to encrypt data at rest and in transit, secure mobile boot and two-factor authentication identified as biggest potential Android security improvements

Desired Security Features

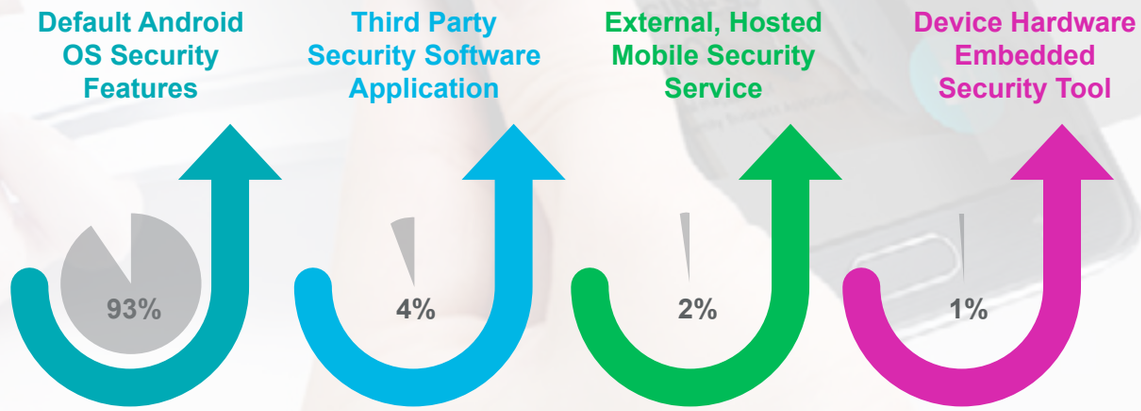
- **On Device Application and Data Encryption** 70%
- **Application Specific Virtual Private Networks** 46%
- **Secure Mobile Boot Capabilities** 44%
- **Single Sign-On/Biometric/ Smart Card User Authentication** 40%
- **On Device Virtual Container to Separate Personal from Business Profile** 36%
- **Integration with MDM Platforms Already Deployed Within the Organisation** 35%
- **Government Agency Validation of Security Solution** 29%

In 55% of organisations, over half of employees use Android devices for business purposes



Android Usage

Most organisations utilise default Android security options rather than third party applications or services



Default Security Options

SAMSUNG

IDG CONNECT

Introduction

Enterprise mobile usage has accelerated sharply over the last five years as the emergence of powerful, large screen smartphones and tablets coupled with a parallel expansion of high speed wireless WiFi, 3G/4G networks have improved employees' ability to access a broad range of business applications and data from wherever they happen to be.

The benefits of that trend in terms of business flexibility and worker productivity are incontrovertible, but it has also presented significant challenges to IT departments responsible for deploying, configuring and managing large numbers of staff issued or owned mobile devices.

The requirement to maintain adequate security on Google Android devices is especially acute given that up to 80% of smartphones shipped in the last few years are pre-installed with the operating system.

A large portion of those handsets are finding their way into business environments, so it is vital that IT departments find ways to protect the integrity of the data stored on, and accessed by, Android devices - more so considering the increased volume of malware and viruses now being targeted specifically at mobile operating systems and the opportunities for unauthorised access due to lost or stolen devices, and unsecured networks those operating systems present.

IDG Connect interviewed around 150 people based in Australia, the UK and the US to build up a more detailed picture of how they approach security provision for Android devices used for business activity within their organisation. All of those polled worked for companies employing 1,000 people or more and 55% over 5,000, with 71% holding IT management related roles such as administrators, directors, chief technology/information/ security officers and business managers and board room executives making up the remainder. The largest contingent (20%) came from the software and computer services industry, followed by key verticals including health, medical and pharmaceutical (13%), finance and investment (11%), manufacturing (9%) and retail (7%).

The results gauge the current scale of their Android smartphone and tablet usage, identifies the applications most commonly accessed and attempts to assess the extent to which enterprises are content to rely solely on the default security tools embedded within the Android OS as standard. It also identifies which additional security mechanisms or services are most likely to be on their wish lists and judges what smartphone and tablet manufacturers are considered to offer more robust platforms for extra protection.

SAMSUNG

IDG CONNECT

Over Half of Employees use Android Devices for Business Purposes in 55% of Organisations

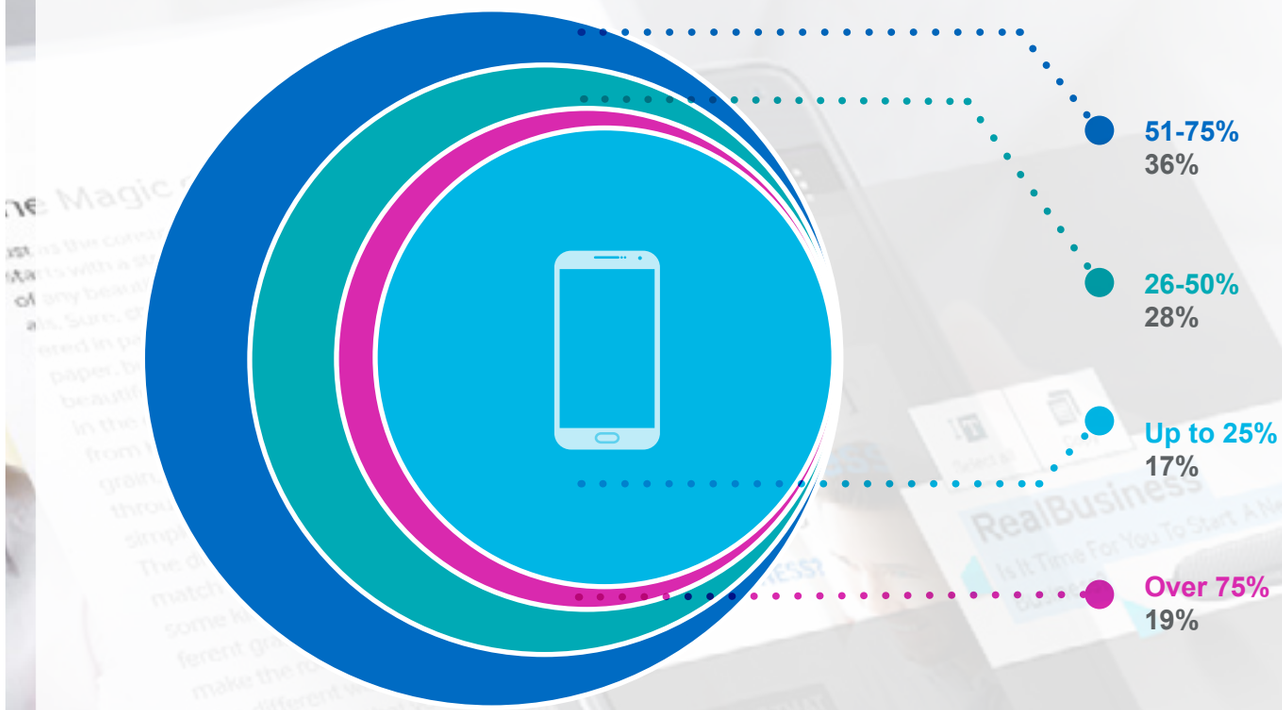
Android smartphones and tablets are widely used for work related tasks across Australia, the UK and the US. Of those taking part in the IDG Connect survey 55% estimated that over half of the employees working within their organisation use them for business purposes as growing numbers of staff look to improve their productivity by remotely accessing data and applications from locations outside of the office.

Almost a fifth (19%) of those polled on aggregate reported large scale rollouts of Android devices to employees, reporting that they were used for business purposes by over 75% of the employees working at, or for, their companies. This number was marginally lower in the US specifically (14%) which conversely recorded the highest number (34%) of organisations where Android devices are used by 25-50% of employees.

The findings confirm that penetration of Android devices is widespread in business environments, with sales forecasts from research company IDC and others indicating that penetration will expand further in the next few years.

IDC estimates that a total of 334.4m smartphones were shipped worldwide in the first quarter of 2015, for example, up 16% from 288.3m year on year, with over three quarters of those devices (78%) being Android smartphones. Research firm Gartner posits similar figures, suggesting that 336m smartphones were sold in Q1 2015, 79% of which were Android devices, though that market share was down almost 2% on Q1 2014.

IDC has also forecast that that global smartphone sales will continue to grow over the next four years, albeit at a slower compound annual growth rate (CAGR) of 5% compared to previous years. Australia, the UK and the US account for a significant portion of global sales between them. IDC's Worldwide Quarterly Mobile Phone Tracker estimates that the US will account for 11.8% of all smartphone sales in 2015, with the UK 2.4%.



SAMSUNG

IDG CONNECT

Application/Data Security and Mobile Device Management Needs Most Likely to Dictate Investment Priorities

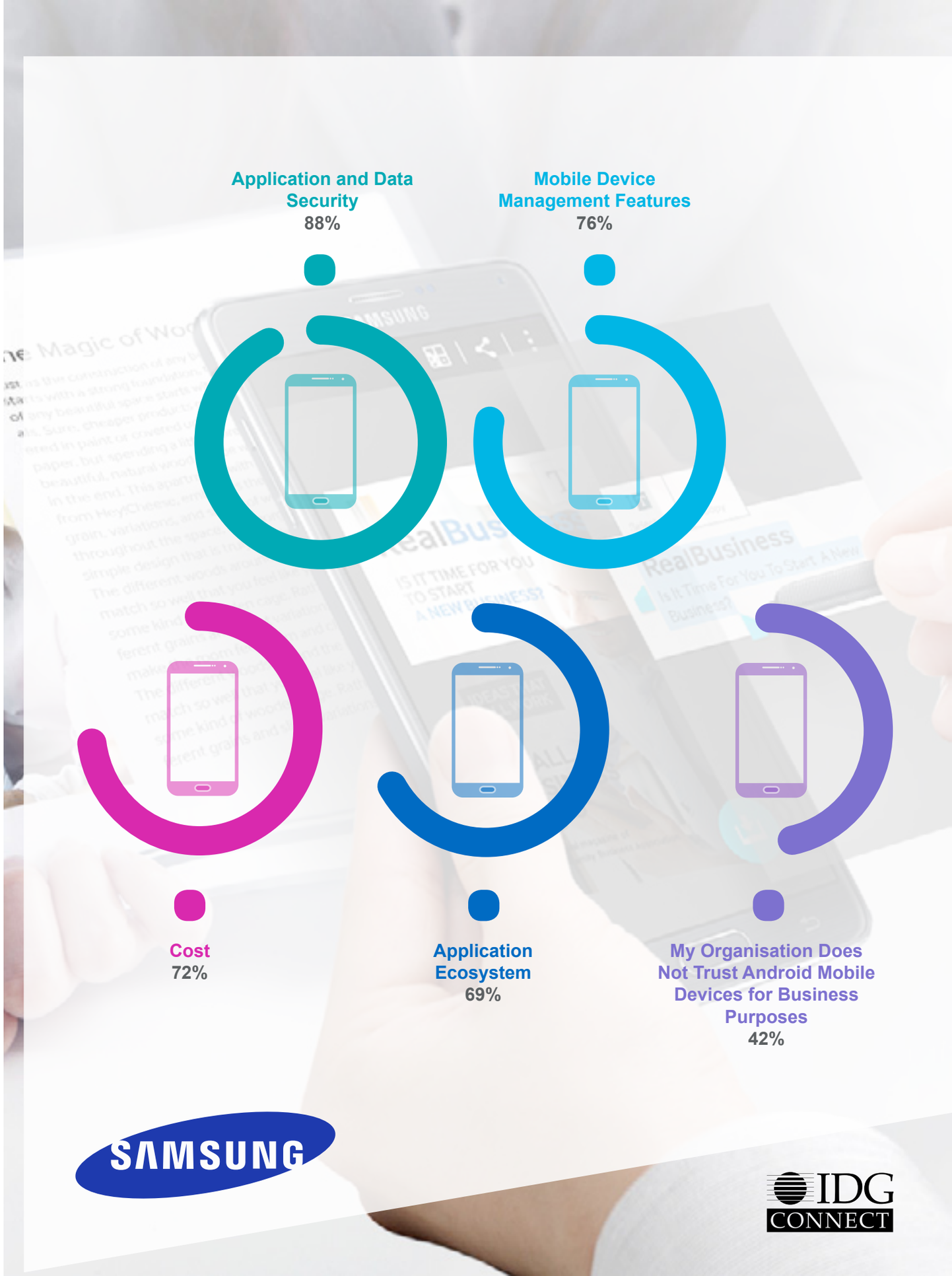
The ongoing need to protect the integrity of sensitive commercial information and user authentication details remains foremost in enterprise buyers' minds when it comes to choosing which mobile devices are deployed across their workforce and/or allowed to access enterprise networks, applications and data stores.

This is reflected in the survey's finding that application and data security is the factor considered most important in influencing any management decision to deploy Android devices for business usage (weighted at 88% by those polled).

Mobile device management (MDM) features (76%), cost (72%) and support for a broad application ecosystem (69%) that provides a wide choice of business software for use on mobile devices are given roughly equal weighting by the survey base on aggregate.

Those same MDM features (82%), cost (80%) and application ecosystem support (76%) are considered more important to procurement strategies by larger companies employing 10,000 people or more, and there are regional differences: fewer people in the UK rate the importance of MDM features (68%) and application ecosystem support (62%) than those in Australia and the US, for example.

Nor is the strong current focus on application and data security likely to change in the future - almost all of those polled (98%) additionally predicted that it would represent the single most important factor influencing investment in Android smartphone or tablets for business purposes two years down the line.



Most Organisations Utilise Default Android Security Options Rather than Third Party Applications or Services

Despite their present and future focus on application and data security, few organisations in Australia, the UK and the US currently employ any security tools beyond those already available within the Android operating system.

When asked to identify one method harnessed to provide mobile security on Android devices used for business purposes, 93% reported that they relied on the default security features built into the OS itself. There was again some regional variation amongst the survey base, with those in Australia showing a preference for both third party security software (8%) and hosted mobile security services (4%) which was slightly above the aggregate.

At face value this finding may suggest that almost all believe that their organisations are satisfied with the level of mobile security protection that the Android OS provides to meet current requirements. But it is also possible that some respondents remain either unaware of the precise features or functions which have been deployed and/or have been given no reason to suppose that their organisation has sufficient motivation to supplement default Android security provision with additional layers of mobile protection using third party software or services.

As we will see later in this paper, the same number (93%) appear vague on whether default Android options security match their business security requirements or not (Tab 10) – another indication that they may not be aware of what those Android security capabilities are, or how they measure up against security frameworks set out by their IT departments.

Ability to Encrypt Data at Rest and in Transit Identified as Biggest Potential Android Security Improvement

In contrast to their acceptance and usage of default Android OS security options as the mainstay of their current enterprise mobile security provision, organisations in Australia, the UK and the US have very clear ideas on how best to harden current Android security protection.

On device application and data encryption is seen as the approach most likely to improve security levels currently implemented on Android devices used for business purposes by 70% of those polled, further identified as the single most important technology by 94% on aggregate. More organisations in the UK rated encryption as particular source of potential security improvement (76%) with 100% additionally considering it most important within two years' time.

The ability to protect data in transit as well as at rest on Android devices is another important priority for many companies, with application specific virtual private networks (VPNs – those that set up encrypted communication sessions with individual remote applications without affecting the operations of other applications) cited as a top three feature by 46% of respondents on aggregate.

The benefits of secure mobile boot capabilities which safeguard sensitive data and user login details stored on Android smartphones and tablets by preventing unauthorised access if they are lost or stolen were also acknowledged by 44%.

Whilst they were cited as a top three feature by a lower number of respondents many of those polled also highlighted single sign on, biometric and smart card authentication tools (40%) as potential areas of Android security improvement, alongside on device virtual containers which separate personal from business profiles (36%) and integration with MDM platforms.

SAMSUNG

IDG CONNECT

Email, Messaging, Productivity Suites and Communications Software Forms Mainstay of Mobile Business App Usage

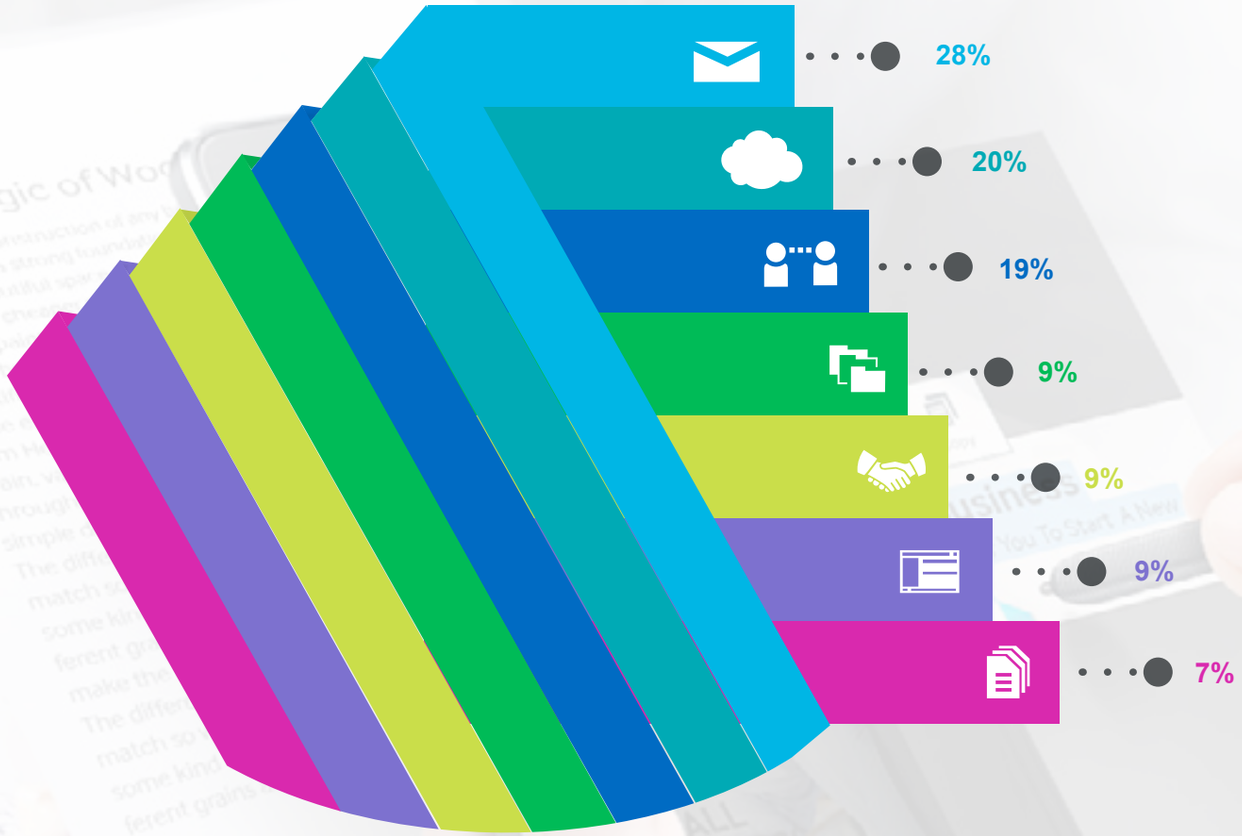
With so many employees using Android devices for work related tasks it is inevitable they will run a broad mix of enterprise orientated mobile software to support their daily activity, and each application is likely to present its own security challenges and requirements.

The most widely used applications accessed from Android smartphones and tablets were reported as email clients and messaging tools (28%), closely followed by cloud based productivity suites (20%), examples of which include Microsoft Office365 or Google Docs, and which both incorporate email and messaging elements of their own.

Communication and collaboration between colleagues, business partners and customers using Android mobile devices is a recurrent theme, with 19% of those polled also indicating organisation-wide use of conferencing tools which may include GoToMeeting, Skype and WebEx.

A smaller percentage also use Android smartphones and tablets to access customer relationship management (CRM) and enterprise resource planning (ERP) applications, traditionally favoured by sales staff who spend large amounts of time out of the office. An equal number (9%) either replicate their entire desktop environment or specific applications by logging into centrally hosted virtual desktop or application images provided by platforms such as Citrix XenDesktop/ XenApp or Oracle's Virtual Desktop Client.

Enterprise IT departments and employees need to bear in mind that these and many other applications are vulnerable to exploitation by hackers and unauthorised users, and take steps to implement appropriate security measures to protect themselves and their organisation from the loss of sensitive commercial information which is often subject to national laws and industry regulation around data protection.



- Email/Messaging Apps
- Cloud Based Productivity Suites
- Communication, Video/Audio Conferencing and Collaboration
- Hosted Virtual Desktop Environments or Applications
- Customer Relationship Management (CRM) or Enterprise Resource Planning (ERP) Applications
- Web Browsers
- File Synchronisation Software

SAMSUNG

IDG CONNECT

Importance of Validating Enterprise Security Solutions Against Government Requirements is Widely Recognised

For many organisations, particularly central or local government departments or their business partners and suppliers, compliance with formal IT security policies which include the mobile devices used by their employees is mandatory.

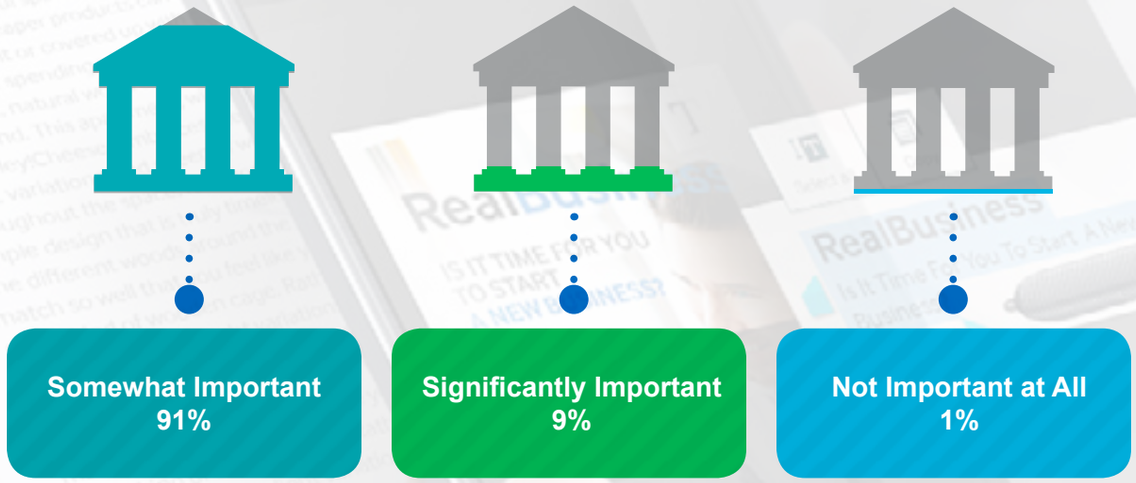
Organisations across the three territories certainly appear to see a clear imperative for matching enterprise security provision against security certification frameworks and/or guidance outlined by government bodies, but this does not take precedence in most cases. The vast majority of those polled (99%) believe it is important to know that any enterprise security solution meets national government requirements such as those set out by the US DoD, Australian ASD or the UK NTAIA for example, but a much smaller number (9%) see this as a priority.

Respondents in the US appear particularly keen on co-operation with government data security certification initiatives with a much higher percentage (18%) reporting this as significantly important, much higher than those in Australia (2%) and the UK (6%).

Relevant data security frameworks in the US include the Defense Federal Acquisition Regulation Supplement (DFARS) which insists that minimum data protection levels be implemented by both US and foreign companies acting as Department of Defence contractors. The Digital Services Advisory Group and Federal Chief Information Officers Council has also issued security toolkit covering bring your own device (BYOD) polices for both federal government agency and the contractors they employ which demand that smartphones and tablets brought onto government premises have appropriate user authentication controls, password policies, remote wipe features and root kit protection.

The Australian Signals Directorate has published advice on risk management for companies implementing BYOD schemes designed to protect against sensitive data being lost or compromised, and approved KNOX enabled mobile devices certified under the Mobile Device Fundamentals Protection Profile (MDFPP) standard for use by Australian government employees to unclassified or dissemination limiting marker (DLM) level. The UK CESG issues security guidance for specific mobile devices to government departments, including those running Android and Samsung KNOX devices specifically.

While the number rating compliance with these security certifications as significantly important is low at 9%, it is important to remember that imperative will vary considerably from one company to another according to a variety of factors, including vertical sector, the precise security requirements of public sector partners, the type of data and applications accessed from employee mobile devices, and the penalties imposed for non-compliance.



Majority of Respondents Ambivalent Towards Default Android Security Options

Despite so many organisations appearing to use default Android OS security features as the sole basis for their enterprise Android security protection policies, it is not clear if these are perceived to offer the best match for enterprise data and application security requirements when used in isolation.

The vast majority of respondents displayed what is best described as ambivalence in this respect - 93% said that their organisations were neither likely nor unlikely to trust default security options alone.

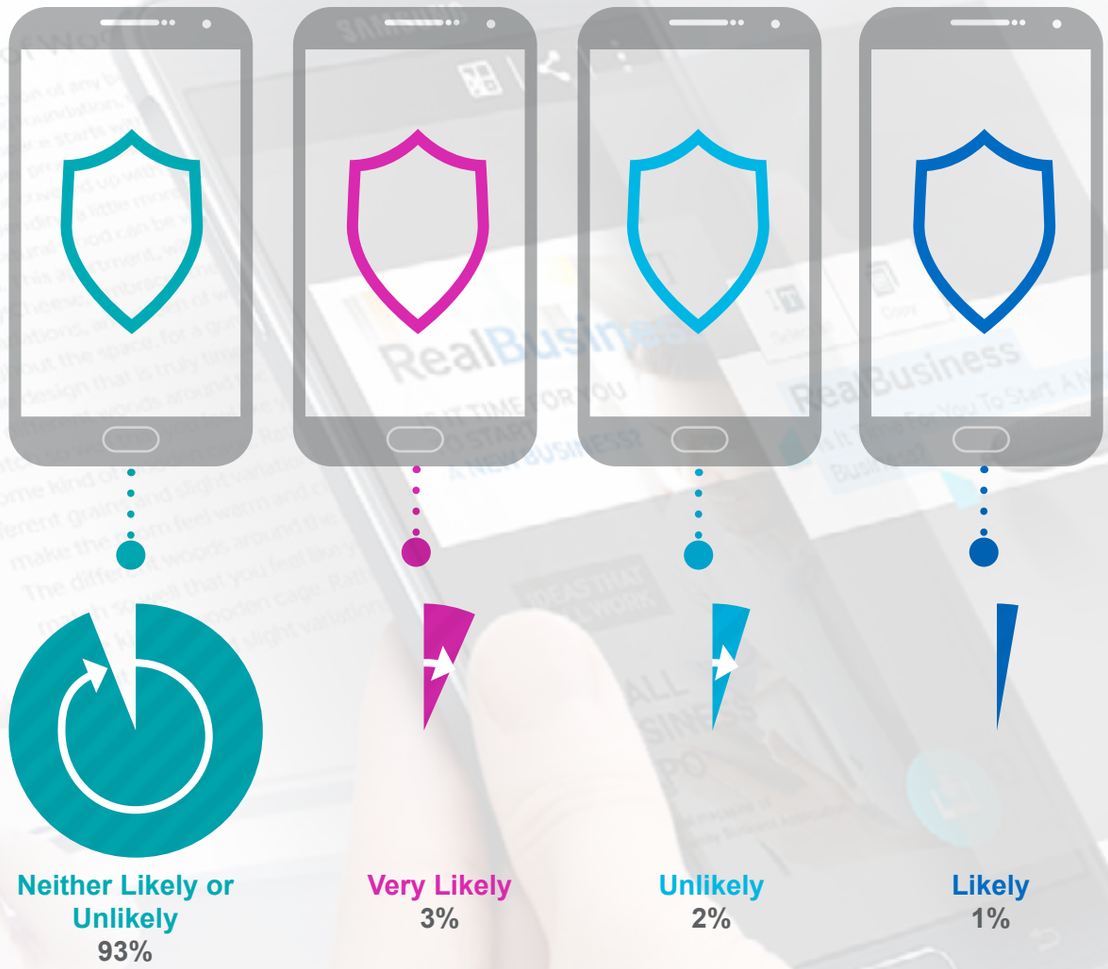
The most obvious explanation for this finding is that those polled are not sufficiently aware of the specific security capabilities available within the Android OS to make a reasoned assessment on whether using them in isolation can meet their organisation's requirements or not, and/or that they may be unfamiliar with the specific security metrics set by their IT departments.

The figure is lower for those respondents from the US (82%), where 10% said they were very likely to trust default Android security options and 6% unlikely, indicating there may at least be a greater awareness of Android capabilities in this territory and the extent to which they match top down mobile security requirements if at all.

The default security options provided in Google's latest Android 5.0 Lollipop OS were upgraded in early 2015, but remain largely focussed on user identification and authentication techniques rather than MDM features, application specific VPNs, government certified security certifications, secure mobile boot capabilities or virtual containers that separate business from personal profiles, for example.

Existing pattern, personal identification number (PIN) and password options have been supplemented with new Smart Lock features that employ facial recognition technology, global positioning system (GPS) technology to link the device's location to the users home or office, and the ability to wirelessly pair the smartphone or tablet with another portable device (such as an NFC tag) to verify the user's identity.

Lollipop also provides remote wipe features and 128-bit AES full disk encryption (FDE) to encrypt all of the user data on the device, though it cannot be applied selectively to specific data sets or applications and relies heavily on the strength of its disk encryption passphrase for its effectiveness.



SAMSUNG

IDG CONNECT

Samsung Considered Leader in Enhancing Android Security Provision

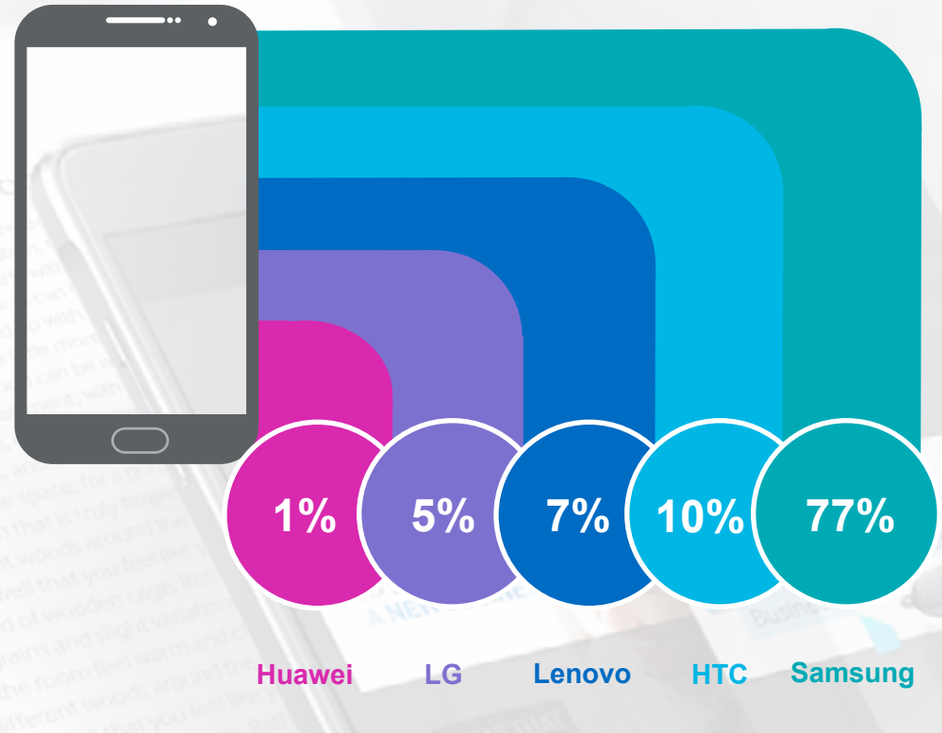
Integral support for additional mobile security capabilities beyond that provided by the Android OS itself varies considerably from one manufacturer to another. Samsung is one company with a strong reputation for building security features into Android smartphones and tablets and is perceived to be a leader in this field by over three quarters (77%) of respondents on aggregate.

Significantly more organisations in the US (92%) see Samsung as a leader compared to those in both Australia (69%) and the UK (70%), whilst Lenovo - which completed its $2.9bn acquisition of Motorola Mobility from Google in 2014 - is rated for Android security by a larger number of companies employing 10,000 people or more (14%) compared to the aggregate figure (7%).

Samsung introduced the first version of its enterprise grade mobile security platform, KNOX, in 2013. KNOX initially incorporated Security Enhanced (SE) Android tools which separated personal and business data and applications into different containers, distributed business profiles and provided data encryption, remote wipe and browser/camera locking functions.

Upgraded in 2014, KNOX 2.0 added additional features which are not found in default versions of the Android OS. These include TrustZone protected certificate management, a universal MDM client and support for fingerprint scanner biometric authentication, split billing, and multi-vendor VPNs integrated with containerisation platform, single sign on directory services, an authorised market place from which employees can download secure apps and customisation options.

KNOX enabled mobile devices have also been approved for use by a range of national government bodies which are particularly sensitive to potential issues caused by lost data and unauthorised system access. These include the US Department of Defence and National Security Agency (NSA), as well as the Australian Signals Directorate (ASD) intelligence agency and the UK Certified Cyber Security Consultancy (CESG) - the information arm of Government Communications Headquarters (GCHQ) and the National Technical Authority for Information Assurance (NTAIA) - which offers security guidance and support to government departments.



Conclusion

Android smartphones and tablets are used extensively for business purposes across Australia, the UK and the US, with 55% of those polled by the IDG Connect survey estimating that over half of workers within their organisation use them to run a broad mix of enterprise orientated software applications, including email and messaging tools, cloud based productivity suites and various communication and collaboration platforms.

That level of mobile device and application usage inevitably demands adequate security protection and safeguarding sensitive commercial data including customer information, financial transactions and user authentication details is the foremost consideration during Android device deployment decisions. Application and data security was seen as the most important factor amongst those surveyed, with mobile device management (MDM) features, cost and an application ecosystem that delivers a broad range of business applications for use on mobile devices also rated highly.

Yet 93% of respondents were unable to provide a definitive assessment as to how likely their employers were to trust the default security options embedded within the Android mobile operating system to support those requirements, suggesting many may have little or no knowledge of precise security capabilities or of any enterprise data and application security obligations set out by their IT departments.

In some cases then, there may well be a gap between current Android enterprise security provision and requirements which third party suppliers - including Samsung which is already recognised as a leader in this field by 77% of those polled - can fill with enterprise mobile security and management platforms such as KNOX.

SAMSUNG

IDG CONNECT