DECEMBER 2013

THE FOLLOWING IS AN EXECUTIVE WHITE PAPER ON:

Enterprise Mobility & Connected Devices

By Eric Klein, Senior Analyst

Android: Ready for the Enterprise

Exclusive License to Distribute:

SOTI®

VDC Research
Insights for the Connected World

Introduction: Android is Ready for the Enterprise

Within the past few years, Android has had a surge of growth in market share, easily beating out the very popular Apple iOS and aggressively taking share away from BlackBerry. In less than three years, Android saw its global market share increase trifold from just above 25% in 2010 to more than 80% globally in 2013. Android's success can be largely attributed to its OEM partnerships and its ability to provide a great user experience at a more affordable price than other competitors.

As Android-powered devices continue to ride the BYOD wave into corporate environments, they have become too significant of a presence for enterprises to ignore. Their dominance in the market has made them a primary target by malware developers. Google has made notable security enhancements to the platform since its launch. VDC anticipates that Android deployments in enterprise settings will increase as mobile-first ISVs have sharpened their focus on the mobile platform and have developed highly secure solutions that have made Android suitable for corporate environments. In addition, handset OEMs such as HTC, LG, and Samsung continue to invest in initiatives to augment the security elements of their hardware. Enterprise Mobility Management (EMM) vendors such as SOTI have attacked Android fragmentation head-on with advanced technologies like Android+ that unify policy management across OEMs and Android versions. As OEMs and EMM providers continue to partner to secure the Android OS, IT executives will continue to add Android-powered devices.

Background on SOTI

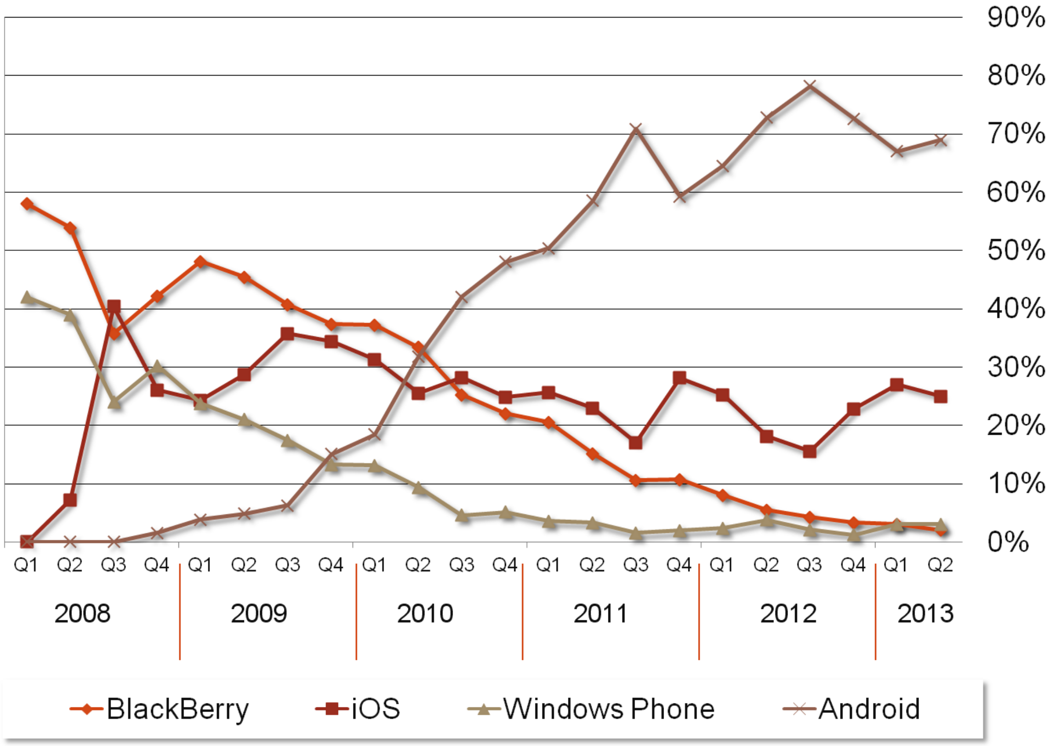
SOTI is the world's most trusted provider of Mobile Device Management (MDM) solutions with more than 12,000 enterprise customers and millions of devices managed worldwide. SOTI develops industry-leading solutions for Enterprise Mobility Management (EMM), allowing organizations to support corporate-liable and Bring Your Own Device (BYOD) policies. SOTI MobiControl solves the unique challenges involved in managing, securing, supporting, and tracking mobile and desktop computing devices across all platforms.

Managing the Risk of Mobility

Mobile device deployments continue to expand in enterprise environments and are being integrated into workers' daily activities in companies of all sizes. For CIOs, CSOs, and IT executives, the explosion of mobile in the enterprise is driving investment in mobile IT management and security. From an IT perspective, the challenge is significant. Protecting data on a server is one thing, but protecting data in motion is another. The increase of mobile devices in the enterprise has us carrying around (and potentially exposing) more information than ever. These days, with BYOD increasing in the workplace, a typical mobile device is likely to contain both personal and work-related data including emails, email attachments, voicemails, text messages, and potentially private corporate data. Essentially, every mobile worker is opening a door into the enterprise network as well as access to confidential data.

While handset vendors such as Apple and BlackBerry have enjoyed success in corporate settings, there has been a notable uptake in Google's Android OS. The Android platform has led the consumer market since Q4 2010 and continues to grow its overall share (see Exhibit 1). While consumer trends are continuing to impact enterprise adoption, the enterprise features that OEMs such as Apple and Samsung are incorporating has these vendors gaining traction in corporate settings. BlackBerry has demonstrated that it has a platform to remain competitive with its recent BB10 release; however, the vendor remains challenged by prevailing market trends and increasing its market share.

Exhibit 1: Market share of mobile OS platforms

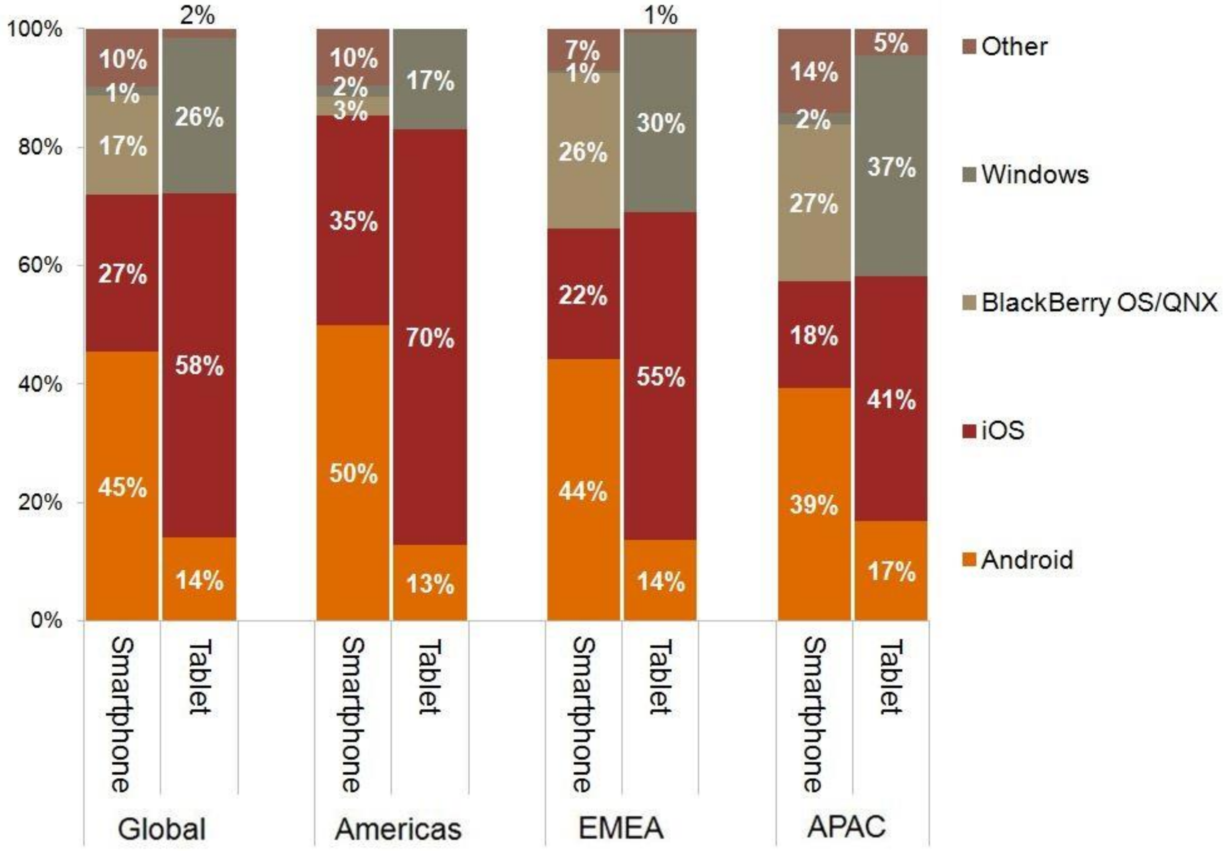


Source: VDC Research, 2013

Android-powered devices continue to ride the BYOD wave into corporate environments and have become too significant of a presence for enterprises to ignore. However, while Android devices are increasingly considered for enterprise use, the well-documented prevalence of viruses and malware on the platform has created a perception problem for Android since its release in 2009. This white paper will explore the reasons behind the growth of Android in the enterprise and how organizations should approach supporting the increasingly popular mobile OS.

There is no question that smartphone and tablet usage in commercial and government organizations is continuing to expand as BYOD programs are adopted. This trend will ultimately impact IT from a support perspective, as the need to support multiple mobile platforms will be required for many deployment environments. Considering the significant variance in device preference by region (see Exhibit 2), organizations that are planning to move forward with BYOD programs should ensure that they invest in a mobile management solution to help manage the risks of mobile enabling their workforce.

Exhibit 2: Regional smartphone and tablet marketshare by OS (2013)

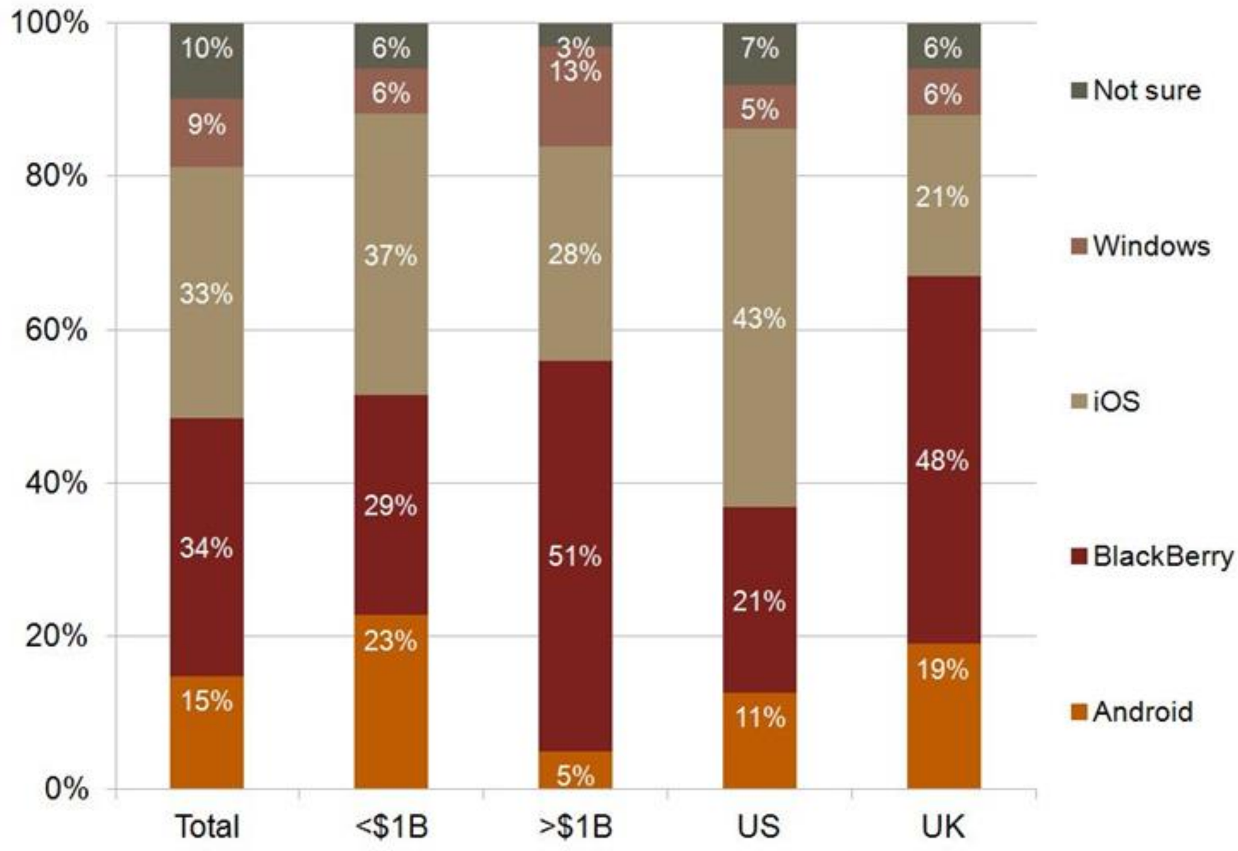


Source: VDC|Research, 2013

Real-Time Antivirus and Malware Protection

According to a recent VDC Research survey, Google's Android OS is perceived as an insecure mobile platform, particularly among larger (>$1B in annual revenue) organizations. When end users were asked which mobile platform users considered the most secure, the open source mobile OS ranked a distant fourth with these organizations, coming in well behind popular mobile platforms like iOS and Blackberry (see Exhibit 3).

Exhibit 3: Which mobile platform do you consider to be the most secure in your deployed mobile environment? (Respondents supporting at least two mobile platforms)



Source: VDC|Research, 2013

Unlike Apple's close curation of its App Store, until recently, Google had largely been content to let the Android developer community self-police the validity of applications made available in Google Play. This laissez-faire approach has played a key role in the amount of malicious code posing as legitimate applications in Google Play. The prevalence of viruses and malware has contributed to Android's perception as an insecure OS in the market. The platform has been a primary target by malware developers since the first Android phone was released in late 2008. To date, Google's attempts to thwart the growth of malware on Android have not been successful. According to a recent report on mobile threats, 96% of all new mobile malware families or variants targeted the Android platform. (F-Secure, Mobile Threat Report H1 2013*).

Google to the Rescue?

With the launch of Android 4.2 this past November, Google embedded a universal app-scanning system into its Google Play Services. This feature, known as Verify Apps, is a significant advancement for the Android platform as it is not impacted by the Android fragmentation due to handset OEM builds or carrier OS updates (the service is automatically available to every device that runs Android 2.3 or higher).

Although many of the exploits are limited to older versions of the Android OS, the bad news is that more roughly 40% of the Android devices in use are on versions prior to 4.0 and, according to Google, 34% of Android users are still on the Gingerbread Android release. Fragmentation will continue as long as handset OEMs continue selling pre-4.0 devices. Many users can't upgrade to the latest OS due to carrier control of the upgrade cycle, which has been slow and inconsistent. There is no question that the addition of the app verification service has helped to improve the security posture of the Android platform. However, additional precautions must be taken into account for corporate deployments, particularly for mission-critical mobile workflows.

The increased adoption of mobile devices into corporate environments has heightened IT awareness of the security risks on mobile platforms compared to traditional desktop computers. With portability, connectivity, and storage capacity, smartphones and tablets pose a significant data leakage risk as they are often being used for personal and enterprise uses. Malware has a well-documented history on mobile platforms, leaving users vulnerable to the risks of identity theft. Malware developers are adept at masking malicious apps as legitimate software in the Google Play store, and code is often executed imperceptibly in apps that appear legitimate to users. A recent report by Trend Micro stated that only 20% of Android users employ any security applications to protect their data (TrendLabs 3Q 2012 Security Roundup*).

Clearly there is a need to defend against the installation of malicious applications, and real-time antivirus and malware scanning is an important capability that organizations must implement to guard against this threat. One best practice to safeguard corporate data is to impose a brief initial quarantine of employee-liable devices before being granted access to corporate resources to ensure any existing malware and spyware is cleansed from the device. Data security policies should include a scan of managed devices at a predetermined interval to detect and quarantine new threats before they spread across devices. EMM software with integrated antivirus and malware scanning is an effective solution to enforce security and provides an additional layer of defense on top of the embedded security mechanisms that mobile OS vendors such as Google and Apple are utilizing to protect their platforms against virus and malware infection.

Android's Way Forward in the Enterprise: Investing in an Enterprise Mobility Management Solution

While BYOD trends are delivering new opportunities for businesses, they also introduce new risks. In order to support device choice, IT organizations need to invest in software and mobile IT infrastructure to protect mobile deployments and manage device and carrier diversity in BYOD environments. According to a recent VDC Research survey, 59% of organizations currently have a formal BYOD policy in place. However, while many organizations are gravitating toward employee-liable deployments, highly regulated and security-sensitive customers will remain loyal to corporate-liable mobile policies due to federal mandates governing data handling such as FINRA (Financial Industry Regulatory Authority), SEC regulations, consumer privacy (regulation S-P), and SOX (Sarbanes-Oxley Act). Regardless of the deployment model, mobile platforms are inherently insecure and require protection via third-party software to minimize the risk from malicious applications, data leakage, and lost or stolen devices.

Moving beyond the common perceptions of the Android OS in large organizations, we see Android as a very suitable platform for corporate environments. Our view is based on our discussions with a broad range of constituents in the mobile ecosystem, including handset OEMs, mobile-first ISVs, and service providers who are implementing mobile solutions in corporate settings. Since the platform's launch in 2008, it has quickly become the most widely used mobile OS for a growing roster of prominent handset manufacturers. While Google has made notable incremental security enhancements to the platform since its launch, mobile-first ISVs are bringing innovative holistic approaches to managing mobile platforms in corporate environments. Market-leading handset OEMs such as Samsung and HTC have invested significantly in initiatives to augment the security elements of their hardware, with Samsung's KNOX technology attracting interest in the enterprise and federal government segments. As OEMs and EMM providers continue to partner to secure the Android OS, IT executives will continue to add Android-powered devices to their approved hardware lists.

Device Management

Mobile security has historically been rooted in management of the device, covering the hardware, operating system, and native applications. Android OEMs including HTC, LG, and Samsung are making significant R&D investments into their management APIs to provide robust security features on smartphones and tablets. Device management remains a cornerstone of security policy for corporate liable devices. The ability to detect rooting or jailbreaking of the operating system, remote lockdown and wipe of the device data, hardware feature controls, and remote control of the device will remain as key features that are requisite to properly protect mobile assets and limit risk in case the device is lost or stolen. But relying on Google's public APIs and OEM APIs is not enough. Google offers very few native management APIs for Android, and not every Android OEM has added MDM API stacks to fill the gap. The high cost and effort of developing and maintaining APIs across a diverse Android landscape restricts most MDM vendors from supporting more than one Android manufacturer. Organizations looking to support Android devices in a corporate liable or BYOD management framework need to carefully consider the breadth and depth of management across Android OEMs before deciding on a solution.

Secure Connectivity

A large part of the value of deploying mobile devices in the enterprise is the ability for employees to connect to enterprise resources on any device, at any time, in any location. Connectivity to enterprise resources including email, databases, and line of business applications is central to this value proposition. Securing connectivity is a fundamental requirement to manage risk of data leakage and unauthorized access. The strategy and policies for managing mobile endpoints should be consistent with those in place for desktop PCs and laptops. The provisioning of VPN access and certificates for each enterprise device is necessary to allow users to securely access corporate resources.

Application Management

The popularity of mobile applications in the enterprise mandates a strong mobile application management (MAM) and security strategy. A focus of a comprehensive MAM strategy is application verification and security, especially in the context of a BYOD deployment. Is the application that a user downloads to a corporate liable device genuine or malicious code? Can the applications on a user's personal device be trusted if the user is given access to enterprise resources in a BYOD policy? The security around applications running on mobile devices is a critical requirement.

Verification of application validity and integrity in the enterprise is critical to maintaining the security of enterprise data. Strategies including jailbreak and rooting detection can prevent users from circumventing OS-level protection and installing unapproved applications. Whitelisting and blacklisting policies are an effective measure for controlling user access to applications readily available in the ecosystem. Implementing a corporate application storefront as a replacement for a consumer storefront ensures that applications are vetted prior to inclusion in the catalog, assuring users that any applications available from the enterprise catalog are secure and approved for use. In industries that have stringent privacy and security requirements such as finance and healthcare, limiting access to device features and applications through a kiosk mode or a custom user interface can be an effective protection against unauthorized downloads and device configuration while ensuring users have access to specific line-of-business applications and device capabilities necessary for their role.

Location Services and Geofencing

The best enterprise security strategy incorporates a layered approach, and a secure mobility strategy is no different. Established measures including corporate firewalls and physical access controls are being extended to mobile devices to ensure the protection and integrity of assets and data, but their utility is limited when the device leaves a physical location. Enterprises are looking to EMM solutions to provide location-based services that leverage on-device assisted GPS (aGPS) capabilities to protect assets. Geofencing is a solution that uses device aGPS or Wi-Fi triangulation and EMM server-side intelligence to control access to corporate content, applications, and services depending on the physical location of the device. Geofencing is an attractive security solution for highly regulated industries that require strict controls for data loss protection. For example, a health care network could institute a geofence around member hospitals to safeguard patient information outside of hospital premises. On a broader scale, federal agencies could employ geofencing as a preventative measure to safeguard data and restrict device capabilities in geopolitically sensitive areas. The increase of mobile enterprise applications and services has increased data residency on mobile devices, introducing a level of risk that eclipses security concerns of just a few years ago that were focused almost exclusively on email. Location-based services add an additional layer of security to manage the risk inherent in providing broad access to enterprise resources across corporate-liable and employee-liable devices.

Secure Web Browser and URL Filtering

Enterprises are acutely aware that unfettered access to the Internet isn't acceptable on desktops, but mobile poses an additional challenge for IT departments. Web access can be managed behind the corporate firewall, but what happens when the device leaves the corporate network and wanders onto an open Wi-Fi hotspot? Realizing that secure browsing functionality must remain resident on the device at all times, EMM solutions need to consider a network-agnostic approach to web filtering. A secure web browser or URL filtering feature that is always on and integrated into the EMM solution is critical to securing the internet experience on the device and preventing access to untrusted URLs that can be an on-ramp for malware on mobile devices. Secure web browsers offer the same rich web experience as the native device browser, employing whitelist and blacklist policies to manage access in accordance with the enterprise's acceptable use policy.

Containerization and Data Loss Prevention (DLP)

BYOD has matured into a mainstream mobility policy in the enterprise. While there is still a healthy chorus of debate on BYOD, employees are bringing their own devices into the workplace and enterprises are supporting them. With BYOD on the rise, it's more critical than ever to secure corporate data on the device – even if the device doesn't belong to the corporation. Data loss prevention (DLP) has emerged as an important priority for CIOs that are considering supporting Android in their BYOD policy. Containerization is one solution that is effective as a DLP control when used as a layered approach to protect against intentional or unintentional disclosure of sensitive data. A container is an encrypted storage space on the device that can be secured and managed independently of the rest of the device. Among Android vendors, Samsung has taken the lead in implementing a containerized solution with their KNOX technology. KNOX uses a secure encrypted Android container on the device to isolate corporate data from personal data at the OS level. No communication between containerized apps/processes in KNOX container and outside, except for certain read-only use cases (containerized apps have read-only access to data outside). Applications can be silently installed and removed in the KNOX container, and the container itself can be remotely administered like a separate entity, with lock, unlock, and selective wipe policies specific to the KNOX container. Advanced security measures including Enterprise Single Sign-On (SSO), Federal Information Processing Standards (FIPS) compliant VPN, and Common Access Card (CAC) support are integrated into the KNOX solution to meet the most demanding security requirements in government, finance, and health care, among other segments. KNOX APIs are essentially dormant on the device and require an EMM solution to unlock the full range of security and DLP features.

Conclusion

Android is ready for the enterprise. Android-powered devices continue to ride the BYOD wave into corporate environments and have become too significant of a presence for enterprises to ignore. Google continues to make notable security enhancements to the platform, which has helped reduce the platform's attack surface. VDC anticipates that Android deployments in enterprise settings will increase as mobile-first ISVs have sharpened their focus on the mobile platform and have developed highly secure solutions, which have made Android suitable for corporate environments. In addition, handset OEMs such as HTC, LG, and Samsung continue to invest in initiatives to augment the security elements of their hardware. As OEMs and EMM providers continue to partner to secure the Android OS, IT executives will continue to add Android-powered devices to their approved hardware lists.

BYOD trends will impact mobile IT investments for the foreseeable future. The line between personal computers and mobile devices continues to blur. However, our research shows that mobile platforms are inherently insecure, with vulnerabilities such as malware, direct attacks, data interception, exploitation, and social engineering rapidly transitioning into the mobile space. This has heightened IT awareness of the security risks on mobile platforms compared to traditional desktop computers and has made investment in third-party software critical to minimize the risk from malicious applications, data leakage, and lost or stolen devices.

Investment in mobile IT and infrastructure is required. In order to support device choice, IT organizations need to invest in software and mobile IT infrastructure to protect mobile deployments and manage device and carrier diversity in their BYOD environments. A variety of approaches are available to enterprises as they expand their mobile deployments and further their mobile initiatives. VDC has identified the following core mobile solution components, which should be considered:

- Secure connectivity to enterprise resources including email, databases, and line of business applications is central to the mobile value proposition and is required for mobile enablement.
- Mobile Device Management (MDM) is foundational and is a cornerstone of security policy for corporate liable devices.
- Mobile Application Management (MAM) verifying and protecting the integrity of mobile applications is critical to maintaining the security of enterprise data. We advise a multi-layered, defense-in-depth approach, and see application management as essential to protect against unapproved applications.
- Containerization has emerged as a powerful method to protect against intentional or unintentional disclosure of sensitive data. Segregating (and securing) corporate data from personal data on BYOD devices is an effective way to mitigate against data leakage.

About VDC Research

Market Intelligence for Technology Executives. VDC Research Group (VDC) provides market research and advisory services to the world's top technology executives. Our clients rely on us to provide actionable insights to support their most important strategic decisions. The firm is organized around four practices, each with its own focused area of coverage including: automatic identification and data collection, embedded hardware, embedded software and enterprise mobility.

For more information about this research, please contact:

VDC Research Group, Inc. | 679 Worcester Road | Suite 2 | Natick, MA 01760
508.653.9000, **info@vdcresearch.com**

VDC|Research
Insights for the Connected World