SOTI®

ENTERPRISE MOBILITY MANAGEMENT

skywire

White Paper

Android for Work powered by SOTI

Work The Way You Live

SOTI

White Paper

Android for Work powered by SOTI

transforms workplace mobility with enhanced security, consistent management and an open framework for innovation on Android.

Executive Summary

Mobility has reshaped the way we work, regardless of role, responsibility, or industry. The consumerization of IT has accelerated a shift towards mobile computing, with mobile applications and services becoming an integral part of enterprise workflows. Employees expect to be able to use familiar technology at work to be productive while maintaining privacy across their personal device. IT protects the corporate technology infrastructure by carefully gating access to enterprise resources using a policy framework that was originally designed for corporate-liable devices.

Often, the tools available to IT dictated that meeting both expectations were not possible - either IT had full control and the expense of employee privacy or employees had unfettered access to corporate resources without the proper management framework to ensure security. Solutions that promised an enterprise partition on the device were not inherently secure because they didn't address security at the operating system level.

Android for Work powered by SOTI MobiControl, is an integrated device management solution from Google and SOTI that makes it easier than ever for organizations to support Android as a part of a bring your own device (BYOD) or corporate owned personally enabled (COPE) device program. The combined solution enables organizations to enable employees with the apps and content they need in a secure, managed enterprise space.

From Business First to Personal First

Less than a decade ago, mobile devices in the enterprise were predominantly corporately-owned and solely utilized for business purposes. Employees slowly began using corporately-owned devices for personal communications (primarily email and voice calls), driving an increase in cost for organizations. The rise of the smartphone precipitated a change in behavior. Employees were now carrying two devices - a corporate-issued device for work and a personal device for personal communication, social networking, gaming, and other services that were restricted on their corporate devices. Employees began requesting enterprise services on the devices that they were familiar with in their everyday lives - and enterprises were beginning to question their corporate-liable device policies from a cost and employee enablement perspective.

Fast forward to today, where many organizations have embraced a Bring Your Own Device (BYOD) or Corporate Owned Personally Enabled model (COPE) to standardize policy around the enterprise use of consumer mobile technology in the workplace.

As the lines between personal and business use have continued to blur, a growing number of users demanded autonomy for their mobile devices. Since the BYOD movement took hold, enterprises have been seeking ways to seamlessly manage devices without personal apps and data affecting corporate digital assets, and vice versa. The first generation of mobile device management solutions were rigidly device-centric, allowing for policy controls that were all encompassing, similar to the corporate-liable solutions that preceded them.

BYOD Challenges

The first wave of solutions addressed critical security requirements but left a series of gaps that restricted the expansion of BYOD beyond a few device manufacturers and form factors.

IT Controls

The explosion of mobile - form factors, operating systems, OS versions, carrier variants is challenging enterprise IT to find new and efficient ways to manage mobile devices within their IT infrastructure. This mobility management can be overwhelming, as IT needs to stay on top of what is entering the enterprise. This can also lead to lack of IT control, as employees are bringing their own devices to be used for work purposes making the enterprise vulnerable to malware and security threats, if not managed properly.

Securing Corporate Data

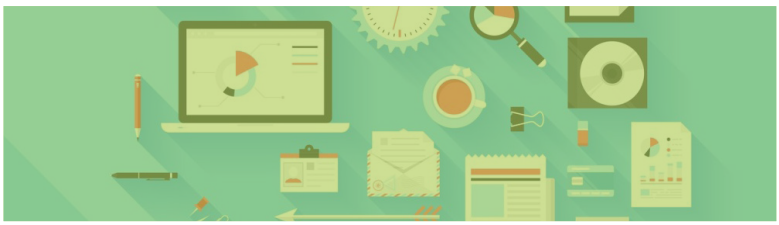
The increased use of personal apps for business purposes is a real threat to data security and a problem that enterprise IT departments deal with on a daily basis. Cloud storage, messaging, and social networking apps are now tightly integrated with today's mobile devices, making them easily accessible, widely available, and widely popular. This acceptance has fuelled their use in the workplace, often at the risk of the security of enterprise data. Enterprise IT has been challenged to find a solution that lets employees use the personal apps they love at work to be productive while maintain security that is necessary to ensure corporate data remains protected. The solutions that have addressed this problem to date have been focused on restricting applications entirely or replacing native device functionality with third-party solutions, degrading the user experience on the device and inhibiting productivity.

A Consistent User Experience

Many solutions that exist impose controls and restrictions at the expense of the user experience, which users often feel is unacceptable on employee-owned devices. Many solutions to date force a user to use a separate application to perform a task rather than the native application that they are familiar with. Users prefer the native experience, part of the reason why they chose the device to begin with. Any solution that tampers with this experience is inherently distrusted by the user, and will not be widely adopted. Enterprise applications were often less than elegant in their execution, which pushed users to consumer applications to get work done.

A Consistent Management Framework

A significant challenge for enterprise IT continues to be the security and management policy frameworks that are fragmented by device manufacturers, at the operating system and version level, and even across carrier variants of the same physical device. Security and management policies were inconsistent and caused the exclusion of a wide spectrum of devices because of the lack of cohesive policy controls. This made it challenging for IT to build policies that offered employees choice, essentially limiting device selection to one or two manufacturers or form factors. Employees with unsupported devices continued to try to circumvent the system and use their personal devices for business use. It's not that enterprise IT wanted to restrict employees from their device of choice - without the proper tools to secure, manage and support the breadth of devices available, they didn't have a choice.



OS Level Segregation of Corporate Data

The first wave of containerization wasn't hardened at the OS level, and lacked the necessary security and data loss prevention (DLP) controls to keep corporate data protected within the enterprise container on the device. Enterprise IT, especially in security-focused and highly regulated industries, required hardware level security with FIPS 140-2 validated 256 bit encryption and secure VPN to protect against unauthorized access and data leakage. Without these policies available natively at the OS level, administrators were reluctant to approve employee owned devices under their corporate security policies. Much like the issue with policy inconsistency, enterprise IT was left no choice - it had to be very restrictive to the devices that were available for BYOD deployment.

The Evolution of Mobile Security

In an era of corporate-liable policy dominance, proprietary operating systems were highly effective in maintaining a secure environment on mobile devices. The restrictive nature of this approach fell short when user preferences shifted to newer, more extensible operating systems like Android for both personal and business needs.

To address security, many IT departments had to turn to third party vendors to provide solutions that involved "containerization" - setting up a separate enterprise space on the device. While successful, it often required altering apps before deployment, adding to the complexity and costs – not to mention the legal hurdles faced with modifications when wrapping ubiquitous apps such as LinkedIn. This has been especially challenging with Android given that each manufacturers' devices has a specific security model. To remedy this, a common framework that separates work from personal data is necessary.

Android for Work powered by SOTI

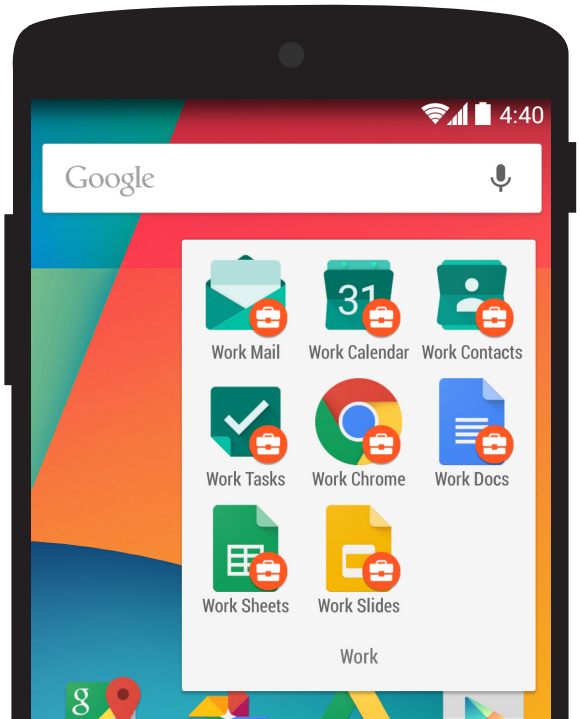
As an approved EMM (enterprise mobile management) solution, SOTI and Android for Work provides all the features needed to manage Android in the workplace. SOTI has long been a leader in Android management, with over 70 Android OEMs certified with its technology – the most in the industry. SOTI's early commitment to Android began with the knowledge that it would in time make major inroads in the enterprise environment as a growing number of users turn to their personal devices
for their work apps.

SOTI and Google leverage their extensive experience in Android innovation to provide best-in-class security and manageability for personally owned Android devices, regardless of the manufacturer. This relationship has been in response to Google's need to bring seamless, standardized EMM support to customers by enabling them to set up Android for Work through SOTI.

With Android for Work powered by SOTI enterprises can take advantage of a dedicated workspace with full operating system level encryption to securely separate business and personal data and applications on employee-owned Android tablets and smartphones. As a comprehensive solution for Android in the enterprise, it includes the ability to:

- Keep corporate data encrypted and secured without interfering with employee personal data
- Activate, manage and remove devices easily and seamlessly
- Provision apps and content safely, easily and securely through a single self-service portal without the need for IT intervention
- Ensure all required apps are installed properly and accessible via the Google Play™ for Work app
- Eliminate the risk of downloading or copying personal apps or data within the secure workspace
- Push configurations over the air to any app built to support it
- Configure Google's native Work Managed Productivity apps - Work Chrome™, Work Docs, Work Slides, Work Sheets, Work Mail, Work Calendar, Work Contacts, Work PDFViewer, and Work Tasks
- Enable full Chrome policy management (e.g. restrictions, URL blacklist and whitelist, proxy configuration and bookmark provisioning)
- Secure VPN support for applications in the Work Profile

Organizations can confidently adopt and support Android devices in the workplace, regardless of who owns the device. Android for Work requires SOTI MobiControl to activate security policies on the device in BYOD or corporate-liable deployments.



BYOD Deployment

For BYOD deployments, Android for Work powered by SOTI provides a dedicated Work Profile on employee-owned Android devices with full OS-level encryption to securely separate business and personal data and applications. Personal data stays private, while corporate data remains secure. A user
can bring their own Android device to work as a part of an approved corporate BYOD program. The user's personal device is enrolled in SOTI and provisioned with a Work Profile that is managed separately from their Personal space on the device. SOTI has no access to the personal space on a user's device, ensuring enterprise data remains secure while protecting a user's privacy.

Corporate-Liable Deployment

In a corporate-liable deployment, SOTI retains full policy control over the device, giving users the familiar Android apps that they need to be productive while retaining strict policy control across the device. A user can be granted a corporate-owned Android device at work as a part of an approved corporate-liable or corporate owned personal enabled (COPE) device program. In this case, the device is enrolled in SOTI and provisioned as a Work Managed Device. As a Work Managed Device, SOTI has full device-wide policy control, ensuring a user is empowered with the applications and services to make them productive while maintaining tight policy controls that are necessary for security-intensive and highly regulated use.

Benefits for End Users

End users, whether they are using a corporately owned or personal Android devices, benefit from a consistent, native experience and the ability to use the Android devices they know and love at work. For BYOD deployments, corporate applications are easily accessible within the Work Profile on the device without affecting the user's Personal space. For corporate-liable deployments, users have the ability to securely use Android devices to be productive without having to sacrifice the native Android user experience.

Your Android, Your Way

With Android for Work powered by SOTI, Android can be used securely at work with the native Android experiences intact, without compromise. IT can silently manage the Work Profile on an employee device, while leaving personal apps and data alone - without the need to use third-party applications or clunky enterprise solutions. Employees are liberated from hard to navigate third-party solutions and can be productive with native Work apps without having to sacrifice the intuitive Android user experience. Android for Work keeps corporate data encrypted and secured, without interfering with personal data. IT has the option to choose choose either BYOD and/or COPE programs to enable access to corporate resources on Android. In the event that an employee decides to change roles or leave the company, the Work Profile can be wiped independently of the employee's personal data.

A New Model for Mobility

Android for Work powered by SOTI enables end-users to work the way they live on Android devices, with secure access to all of the applications and services they know and love.

All The Apps You Love

Mobile apps are changing business the same way they have changed our personal lives - by allowing us to be more efficient and more productive, with an enjoyable user experience.
With SOTI MobiControl and Android for Work, employees can bring the apps they love to work without fear of recrimination from enterprise IT. Leveraging the depth and breadth of apps available on Google Play, IT can provide a curated app experience that is aligned to your organization, keeping personal apps separate.

BYOD is IT Friendly

IT can give the green light to employees - go ahead and bring your Android devices to work. With SOTI powering Android in your workplace, IT has got your back. For employees, the days of going rogue are over. With IT including Android devices in their managed mobility policies, employees are free to choose the Android device that suits their needs without fear of IT recrimination or limited support for corporate apps and services. Employees can simply enroll personal devices securely to SOTI MobiControl without giving access to any of their personal data, and have the ability to add or remove devices conveniently without needing to make a trip to the IT helpdesk.

Benefits for Enterprise IT

With Android for Work powered by SOTI enterprise IT benefits from a unified framework to enable, optimize and secure Android devices independent of operating system version, form factor, or device manufacturer. IT can silently manage corporate resources on corporate or employee-owned devices, while leaving personal apps and data alone. In the event that an employee decides to change roles or leave the company, IT can wipe the Work Profile on the device independently of the user's personal space, protecting the user's personal data and respecting their expectations of privacy.

Fast Track your Android Deployment

SOTI allows enterprise IT to deploy Android devices with no complex configuration or implementation required. Corporate email, contacts, calendar, apps and security policies are provisioned over-the-air to the device seamlessly without user intervention. Whether your organization is deploying corporate-liable Android devices or allowing employees to use their own at work, SOTI allows IT to get Android devices activated in seconds so employees can get to work faster than ever before. Manageability is simple, with one single agent instead of a multitude of OEM specific agents to worry about. For BYOD, IT can focus on supporting the secure Work Profile on the device confident that corporate data is segregated and protected from the user's Personal space.

Benefit from the Best Tools

IT benefits from the years of Android innovation and expertise. Innovative SOTI features like Geofencing, Policy Alerts, and Reporting seamlessly integrate with Android for Work, allowing IT administrators to manage the end to end Android deployment based on extensible location, device, and user policies. Administrators can activate and manage the OS-hardened Work Profile on Android devices, allowing seamless provisioning of employee devices with apps, content and PIM (Email, Contacts, Calendar) safely, easily and securely. With support for advanced security policies including device attestation and VPN, IT can confidently deploy Android with peace of mind that corporate data will remain protected.

Offer Choice Without Compromise

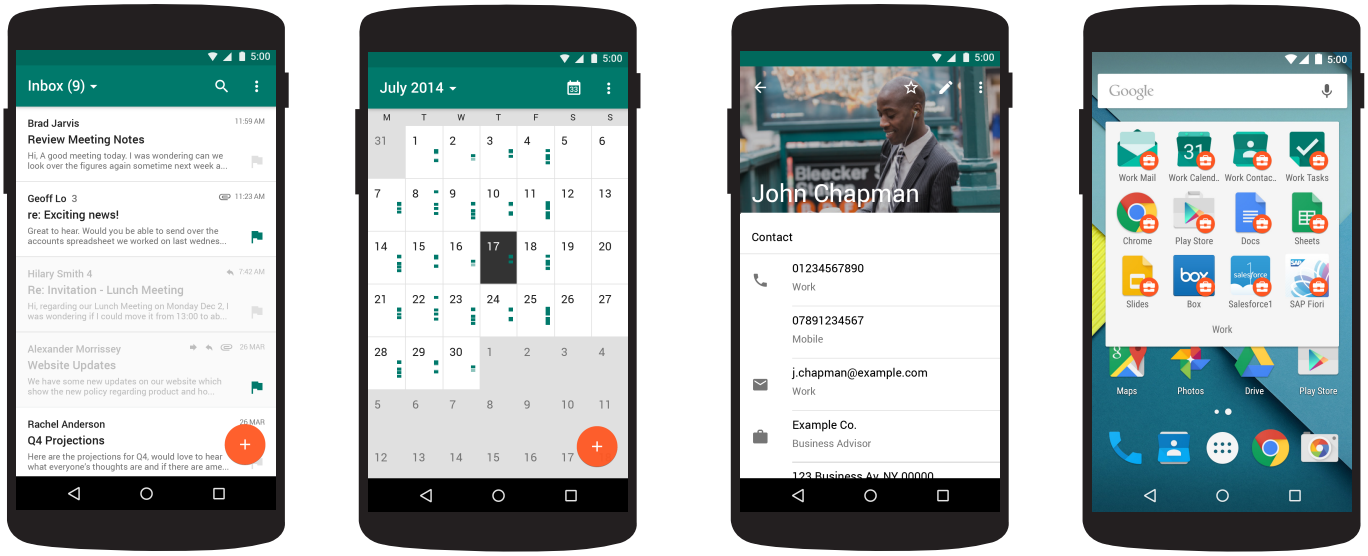
With Android for Work powered by SOTI, IT can confidently manage Android across a broad device ecosystem, offering users the freedom to use their device of choice while maintaining full control over the protected Work Profile. Enterprise can now easily add Android devices and be assured that they are secure within the workplace, regardless of OS, form factor, or device manufacturer.

Security and Privacy Together

Employees are assured that the privacy they expect on their personal device is intact, with virtually zero access to a user's Personal space. All corporate data is housed within a separate and secure Work Profile that cannot be accessed by Personal apps. IT administrators have full control over the Work apps that are available inside the Work Profile without impacting the user experience on the device

Work The Way You Live

The rate of mobile devices coming into the workplace is rapidly driving the need for secure enterprise mobility management. The tools being used on platforms like Android is now outpacing enterprise technology. Mobile is the way we work and live, and balancing both is made possible with Android for Work, powered by SOTI. This ability to seamlessly manage your IT mobility management from a single-pane of glass while taking advantage of a common API framework across all Android devices will transform your workplace mobility with the flexible framework of the world's most popular mobile operating system and the world's leader in enterprise mobility management - Android for Work, powered by SOTI.



SOTI is a proven product innovator and EMM Industry leader. Over 16,000 customers across 170 countries rely on SOTI for their EMM needs. We empower the enterprise to take mobility to endless possibilities.

SOTI.net

SOTI®