SAMSUNG

White Paper:

Transitioning From BlackBerry®

How to Achieve Best-in-Class Mobile Security With Samsung Knox

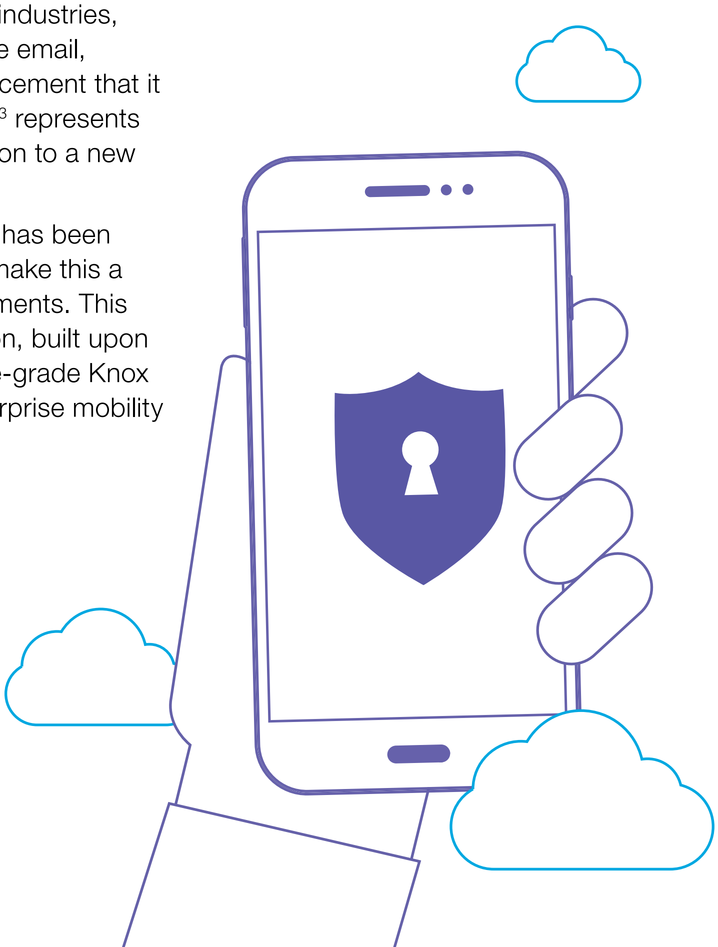
Table of contents

Introduction: The Need for a New Secure Mobile Platform

Just as they have reshaped most aspects of our daily lives, smartphones and mobile apps have also become key tools that employees use to get work done. According to a 2016 study by Frost & Sullivan, employees say smartphones increase their productivity by 34 percent and save them nearly one hour each day.[1] However, for IT leaders whose primary directive is to secure and protect data within government agencies, financial firms and other regulated enterprises, finding a balance between security requirements and employee demands for mobile devices has posed a significant challenge.

For nearly a decade, BlackBerry®'s iconic devices and mobile enterprise ecosystem was the preferred choice of IT decision makers in these industries, providing employees with secure and controlled access to corporate email, messaging and applications. As such, BlackBerry®'s recent announcement that it will outsource the manufacturing of devices[2] and "pivot to software"[3] represents the end of an era, and will accelerate plans by enterprises to transition to a new secure mobile platform.

To address the needs of existing BlackBerry® customers, Samsung has been working closely with BlackBerry®, VMware AirWatch and others to make this a positive, seamless transition — both for device users and IT departments. This white paper will examine Samsung's enterprise-ready mobile solution, built upon the company's industry leading Galaxy device portfolio and defense-grade Knox security platform, in combination with these partners' powerful enterprise mobility management (EMM) solutions.



Chapter 1:
IT and End User: A Mobile Tug-of-War

While BlackBerry® has maintained a strong presence in government, finance and within other security-minded organizations, its share of the broader mobile market has continued to decline, with devices running the BlackBerry® OS representing just 0.2 percent of mobile phones shipped in the fourth quarter of 2015, according to Gartner.[4] With this diminishing scale, the company has struggled to keep up with the rapid pace of innovation in the consumer-driven mobile market, and its smaller user base means the BlackBerry® application ecosystem has grown more slowly than that of Android.

In a 2015 survey conducted by Computing, BlackBerry® had the greatest disparity between IT and end users' overall satisfaction levels with any mobile platform, with 61 percent satisfaction for IT and 44 percent for end users.[5] This disparity is representative of the tug-of-war between IT departments who seek control and easy management of mobile devices, and end users who want the freedom to take advantage of on-the-go productivity applications and expect the same intuitive experience on their business smartphones that they enjoy on their personal mobile devices.

Satisfying Security and User Experience Needs

Samsung has been the leader in the smartphone industry for the past five years; its portfolio of Android-powered Galaxy smartphones is credited with introducing numerous innovations for consumers and business users. Four out of every five smartphones purchased in 2015 ran on Android — a large majority of which were Samsung devices.[6] The Android OS has also attracted a wealth of application developers, with more than 2.2 million apps[7] now available on the Google Play store.

Mobile Device Leader
Knox Security Platform and Solutions
Seamless MDM Partner Integration
1

While devices running the Android operating system may initially have been viewed as vulnerable from a security perspective, Samsung and Google have partnered closely to strengthen security protections at the device, operating system and application layers.

In the same Computing survey, devices on the Android platform achieved a 73 percent IT satisfaction rate, the highest of any platform.[8] The end-user satisfaction rate was 63 percent, a full 19 percentage points above BlackBerry®.

Much of this is the result of Samsung's investment in the Knox platform. Introduced in 2013, Knox is a multilayered security platform that is grounded in the hardware of Galaxy smartphones and tablets. Built on the principles of Trusted Computing, Knox ensures that the integrity of the device cannot be undermined, with a secure vault for security certificates and encryption keys, and hardware-based security for remote access and wireless connections. In a recent comparison, Gartner rated Samsung Knox as the platform with the most "Strong" ratings of any mobile platform, including BlackBerry®.[9]

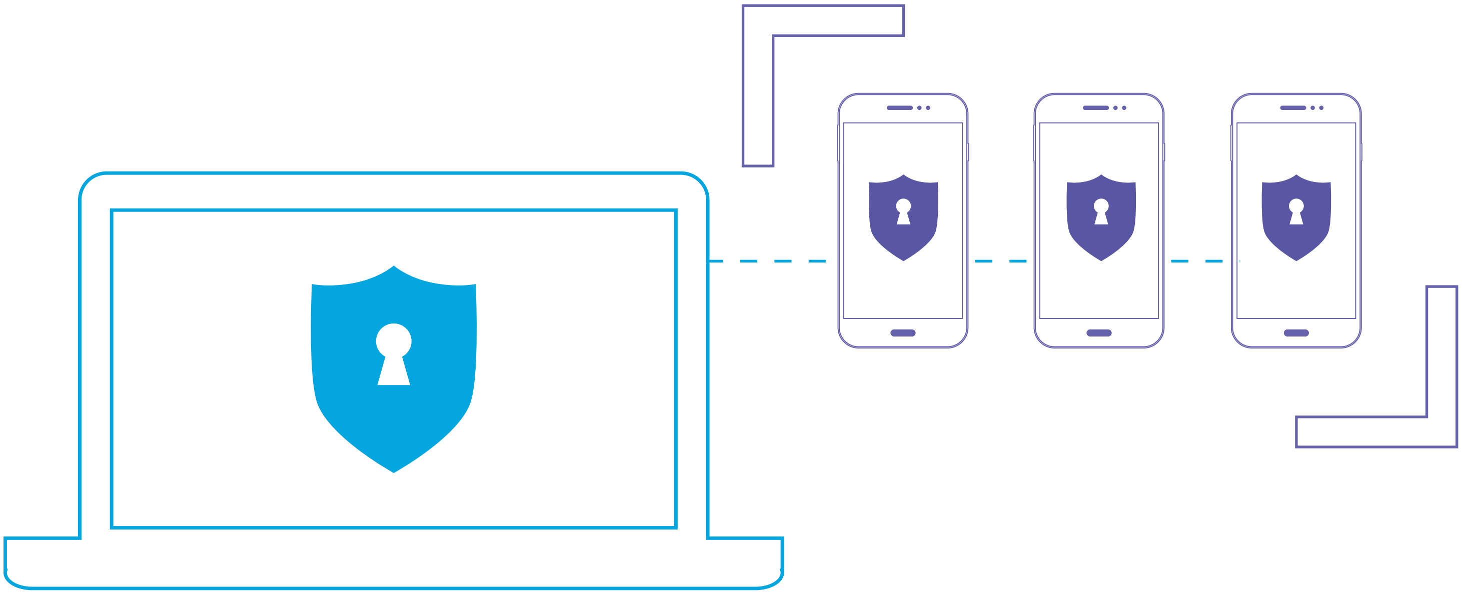
The built-in Knox platform is complemented by a number of optional security products, including Knox Workspace, a containerization solution that allows IT to separate and secure enterprise data and applications on employees' devices.

Partnering to Create an Integrated Solution

Perhaps most important for enterprises preparing to transition from BlackBerry® to a new platform, Samsung has also partnered closely with BlackBerry®'s enterprise mobility software team, as well as other leading EMM providers to ensure tight integration with the Knox platform and products. This allows Samsung Knox devices to integrate with existing BlackBerry® infrastructure, such as the BES12, as well as provide highly secure authentication methods, encryption management and application vetting.

For regulated industries such as government and finance that are concerned about security but also want to meet workers' preferences for consumer-oriented devices, Samsung mobile devices now provide a fully integrated solution. These devices include the highest level of security and manageability features on the market, coupled with a consumer-oriented experience that can boost productivity and increase end-user satisfaction.

To help security-minded IT departments better understand why transitioning from legacy BlackBerry® devices to Samsung mobile devices is the best option, we will now look at the Knox platform's ability to secure data, manage applications and increase end-user satisfaction and productivity.



Chapter 2: Samsung Knox: Defense-Grade Security

Financial services, government organizations and other regulated industries require the highest level of data security. Recent research by Bitglass shows that 81 percent of financial services organizations are worried about data leakage.[10] As the risk of a breach continues to rise, these concerns are valid.

In 2015, at least 87 breaches were reported in the financial services sector, up from 45 in 2014. In the first half of 2016, 37 breaches were disclosed.[11] Over the last several years, one in four breaches in the financial services sector resulted from lost or stolen devices, and another 14 percent were due to unintended disclosures, such as an accidental external share or email,[12] making it critical for financial organizations to secure business-related data on mobile devices.

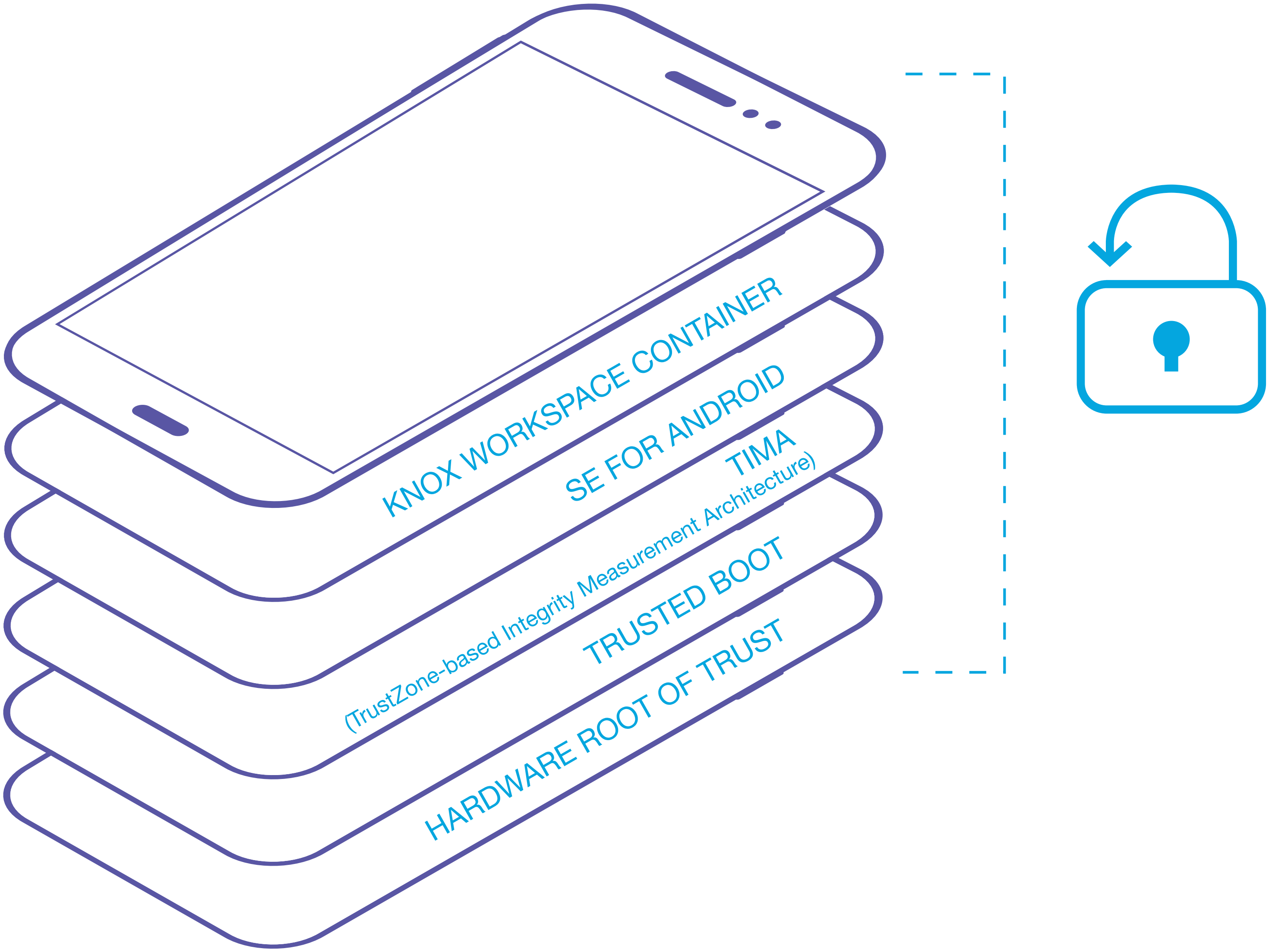
For government organizations, a mobile device's ability to meet defense-grade security requirements, including specific security certifications, is non-negotiable. This leaves government organizations looking for a mobile device vendor that not only holds requisite certifications but also stays up-to-date and achieves new certifications as needed.

While BlackBerry® has long been seen as the leader on this front, with its secure messenger app and end-to-end encryption protocols, the Samsung Knox platform not only meets but in some cases also exceeds the amount of certifications and the levels of certifications that BlackBerry has. Furthermore, Samsung has shown a strong commitment to continuing to meet the highest security standards, including becoming the first to be certified to handle classified government data.

In the Gartner report previously mentioned, Samsung Knox was the only platform to receive "Strong" ratings in all security controls listed in the Corporate-Managed Security category. Gartner rated Samsung Knox as "Strong" in critical categories such as authentication methods, encryption management and application vetting.[13]

A Secure Mobile Workspace

Unlike other Android devices, Samsung mobile devices provide multiple layers of security encompassing both hardware and software. Samsung's Knox Workspace container solution offers additional security, allowing IT to manage and secure corporate data and restrict usage of enterprise apps in a secure workspace separate from employees' personal data. This allows employees to have private access to personal data and apps, addressing personal privacy concerns while still allowing IT to have complete control over corporate data. IT can remotely wipe all business-side data if a device is lost or stolen and make customized decisions about access to applications, such as giving C-level employees access to enhanced productivity features while limiting other employees' access.



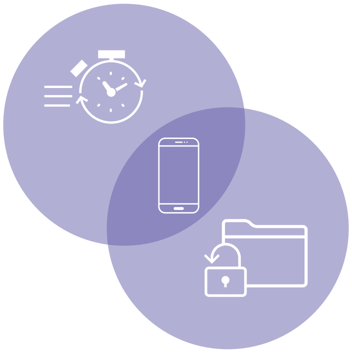
Chapter 3:
Comprehensive Management Capabilities for Granular Control

In addition to securing data, security-minded organizations need the ability to manage mobile security on a granular level. Historically, many IT leaders in regulated industries have turned to BlackBerry®'s Enterprise Server (BES), which is encrypted with end-to-end security while offering greater granularity and security controls than available on iOS or Android.

Now, Samsung makes manageability on an Android platform simple and highly secure by ensuring tight integration between its Knox platform and leading EMM providers. For those IT departments still on BES10, getting the highest levels of security will require an upgrade, but once the upgrade is complete, the Knox platform can integrate with the BES12 or another top MDM solution to deliver essential manageability features.

Streamlining Device Enrollment to the MDM

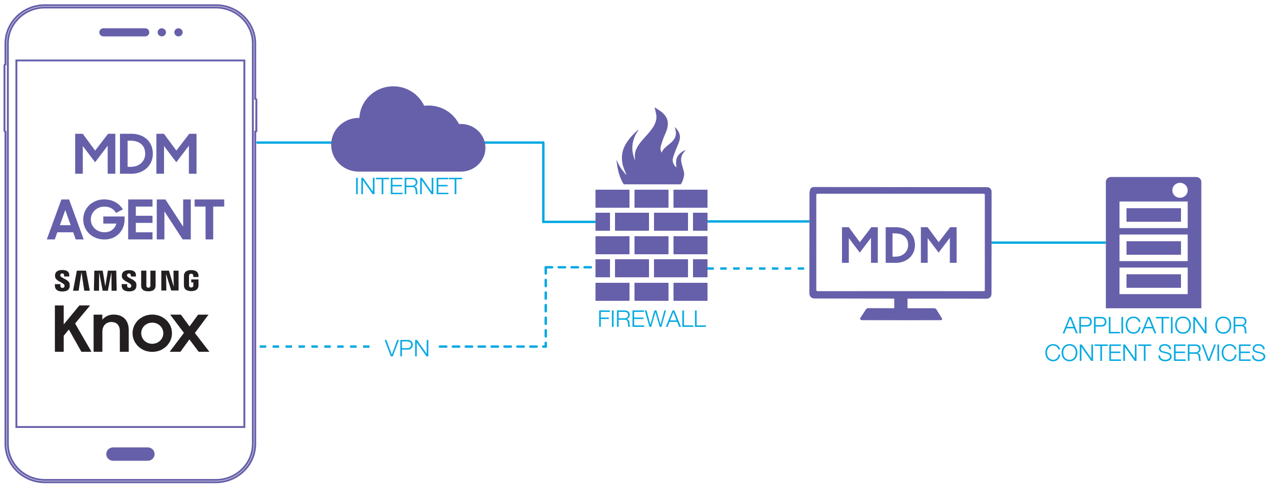
The Knox technology management stack begins with its Knox Mobile Enrollment program, which allows IT to bulk purchase and activate mobile devices through Wi-Fi or LTE. This program saves IT and end users significant time by sidestepping a manual enrollment process and can also save on IT labor costs required to help end users manually enroll. Once a device is enrolled, IT's existing MDM policies are enforced on the end user's device through a zero-touch configuration.

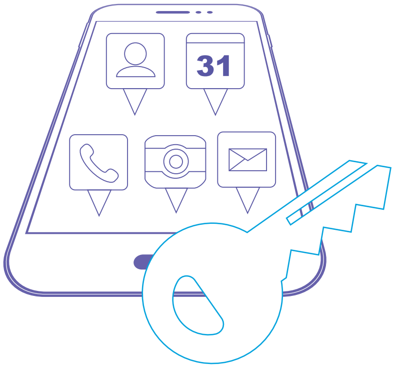


Integration With Mobile VPN Solutions

In addition, Knox can utilize some MDM-provided VPN solutions, such as BES12 or AirWatch Tunnel, to eliminate the need for a third-party VPN vendor. Once again, this feature saves IT time and provides a cost savings on VPN licenses. Samsung Knox also allows for Proxy. Pac for HTTP/HTTPS over VPN to optimize the network and allow IT more granular control of internet browsing on user devices without overloading the proxy server. This solution helps manage high volumes of internal and external server requests rapidly without sacrificing security.

Knox allows for further manageability features through MDM providers or third parties. With SMS/MMS/call log archiving for text and voice conversations, calls can be natively archived according to regulatory requirements in industries such as finance and government. Knox also enables enhanced security and authentication options for intranet and SharePoint through its S-Browser support for NTLMv2 authentication.





App Management With Google Play for Work

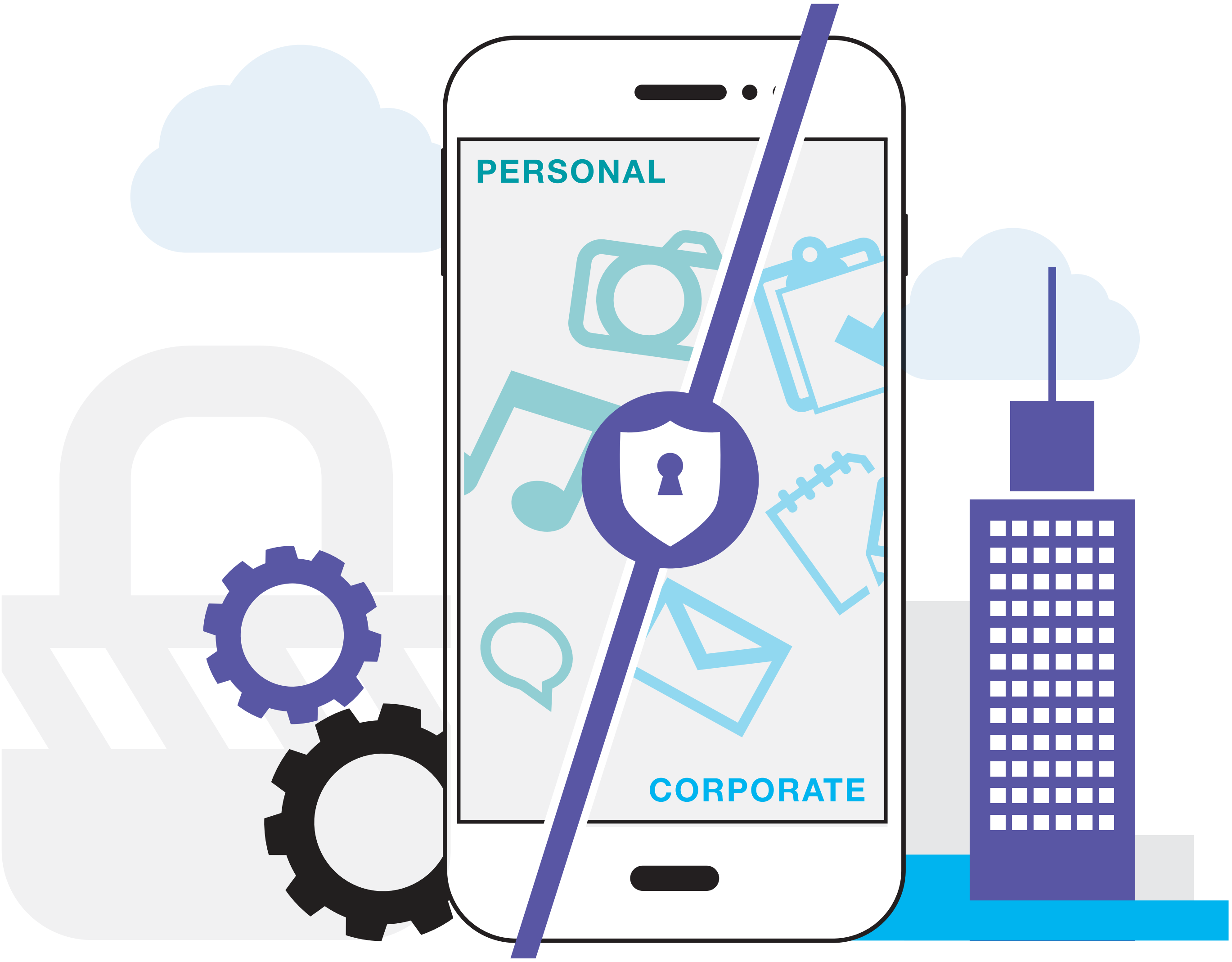
Providing employees with access to the right apps is key to unlocking productivity, but the wrong apps installed on employee devices represent a significant security threat. Integration with Google Play for Work enables the seamless curation of apps by user profiles inside the Knox Workspace. IT can create a customized list of approved apps based on specific profiles for employees to download, apply app configurations and prevent the installation of apps from unknown sources. This is a critical application management capability; research indicates that 66 percent of mobile workers have downloaded and used mobile apps that have not been approved by their employers.[14]

Integration with Google Play also provides access to an extensive array of third-party enterprise apps, including Salesforce and SAP, and enables the secure and private distribution of internally developed apps. Finally, Google Play integration simplifies app management through bulk purchase licenses, allowing IT to transfer licenses to individual users and automatically apply updates.

Booting Directly to Knox Workspace

Finally, Samsung mobile devices provide IT with greater control over employee access to applications on the Android platform. Samsung's direct boot to Knox Workspace allows IT to create business-only devices where employees have access to applications and data only within the Workspace container. This solution works well in a corporate-liable or CYOD (choose your own device) environment where IT maintains control of the device type and access to applications. However, in BYOD (bring your own device) or COPE (corporate-owned, personally enabled) environments, Samsung devices equipped with Knox can offer a dual-persona option, in which corporate data remains locked within the Workspace container and personal data remains outside the container — giving employees the ability to use one device for both personal and work purposes. Additionally, to create a seamless user experience, certain applications within the Workspace container can be granted read-only access to data outside of the container, such as personal contacts, calendar or email.

Knox's integration with top MDM providers, coupled with its integration with Android, gives IT high security and granular control of the devices while creating a familiar and seamless end-user experience.



Chapter 4:
Greater Flexibility and Productivity

In a Computing mobility review, 60 percent of respondents named increased efficiency and productivity as the main benefit of mobility.[15] While regulated industries must keep security in mind, they recognize that the main benefits of their investment in mobility solutions are productivity and efficiency gains.

Respondents in a recent Frost & Sullivan survey report that by using smartphones to get work done, they gain nearly:

58 minutes
of work time each day

58 minutes
of personal time each day

34%
higher productivity[16]

Additionally, 42 percent of respondents said mobile devices helped increase the speed of innovation, provide greater flexibility (41 percent), improve the quality of collaboration (39 percent), boost productivity (39 percent) and enhance the quality of their work (35 percent).[17]

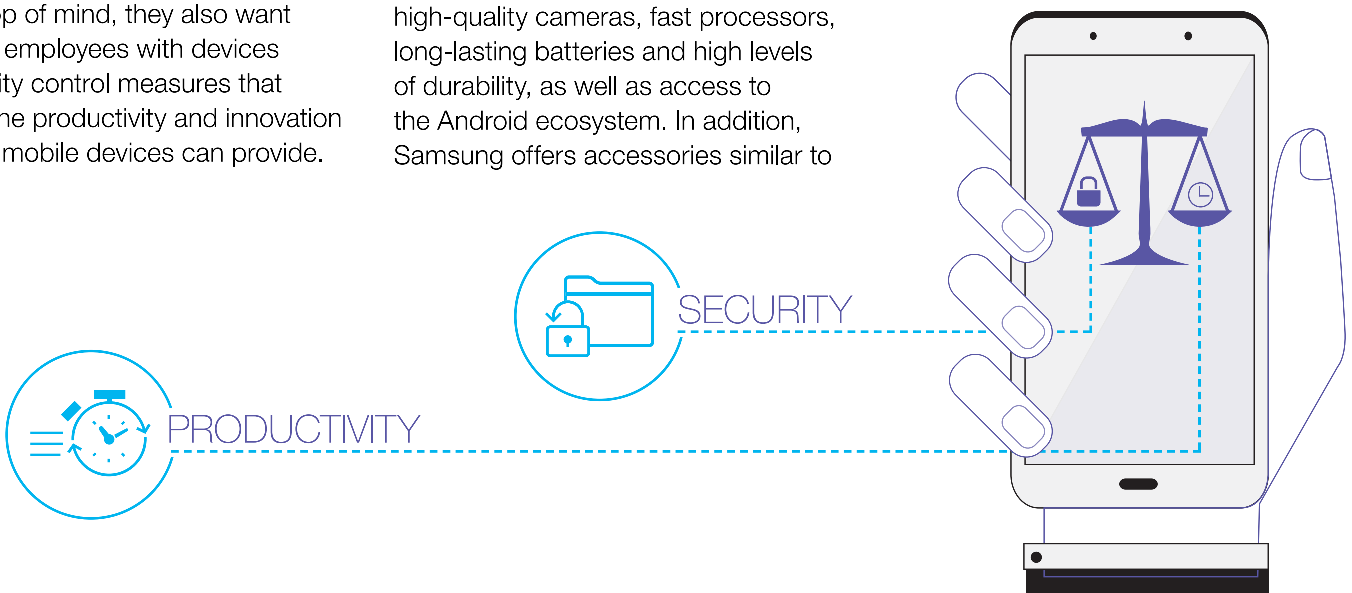
Achieving the Right Balance

While IT decision makers in highly regulated industries must always keep security top of mind, they also want to provide employees with devices and security control measures that enhance the productivity and innovation gains that mobile devices can provide.

Samsung mobile devices provide end-to-end security while offering a range of best-in-class mobile devices with broad consumer appeal that are a leading choice in the consumer and business markets.

In addition to creating a native experience that is familiar to employees, Samsung mobile devices come equipped with performance features that enhance end-user productivity, including high-resolution screens, high-quality cameras, fast processors, long-lasting batteries and high levels of durability, as well as access to the Android ecosystem. In addition, Samsung offers accessories similar to the traditional productivity features of the BlackBerry® devices, such as tactile keyboards.

By making the switch to Samsung devices, IT can maintain stringent security protocols, gain granular management control and still allow employees to increase their productivity with a device that delivers the same intuitive experience they enjoy on their personal devices.



Conclusion:
Keep Security High and Boost Productivity

Samsung Knox devices provide a fully integrated solution that can immediately deliver the secure, manageable stack that's required in regulated industries such as government and finance, while simultaneously offering end users a leading brand choice for a productive, feature-rich device on which to get work done.

The Samsung Galaxy smartphone portfolio offers best-in-class mobile devices that are immediately ready for action and that your employees want to use. Samsung devices come standard with the Knox platform built into every device, offering defense-grade security that protects sensitive data from the chipset to the application layer. It's also trusted worldwide to handle confidential information, including U.S. government-classified data, while offering more management control through tight integration with top MDM solutions.

By making the switch to a Samsung mobile device, organizations will not only maintain the highest level of security and manageability but also garner higher end-user satisfaction and productivity. No other mobile device on the market can meet this promise.

To find out more, visit samsung.com/devicereplacementsolution

Sources:

1 "Employees Say Smartphones Boost Productivity by 34 Percent," Frost & Sullivan Research, Samsung Insights. August 3, 2016.

2 "BlackBerry® Stops Making Phones," Bloomberg Markets. September 28, 2016.

3 "BlackBerry® Reports 89% Year over Year Growth in GAAP Software and Services Revenue for Q2 Fiscal 2017; Company Announces New Strategic Direction for Mobility Solutions," BlackBerry®. September 28, 2016.

4 "Gartner Says Worldwide Smartphone Sales Grew 9.7 Percent in Fourth Quarter of 2015," Gartner. February 18, 2016.

5 "Enterprise Mobility Review 2015," Computing. July 2015.

6 "Smartphone OS Market Share, 2016 Q2," IDC. August 2016.

7 "Number of apps available in leading app stores as of June 2016," Statista. June 2016.

8 "Enterprise Mobility Review 2015," Computing. July 2015.

9 "Mobile Device Security: A Comparison of Platforms," Gartner. April 6, 2016.

10 "Report: How Forward-looking Industries Secure BYOD," Bitglass. 2015.

11 "Financial Services Breach Report," Bitglass. 2016.

12 Ibid.

13 "Mobile Device Security: A Comparison of Platforms," Gartner. April 6, 2016.

14 "The Security Impact of Mobile Device Use by Employees," Accellion and Ponemon Institute. December 2014.

15 "Enterprise Mobility Review 2015," Computing. July 2015.

16 "Employees Say Smartphones Boost Productivity by 34 Percent," Frost & Sullivan Research, Samsung Insights. August 3, 2016.

17 Ibid.

Learn more: samsung.com/business | insights.samsung.com | 1-866-SAM4BIZ
Follow us: youtube.com/samsungbizusa | @SamsungBizUSA

SAMSUNG

WHP-HHP-BLACKBERRYTRANSITION-OCT16SW