Stratecast | FROST & SULLIVAN

BYOD Done Right is a Win-Win for Workforce Mobility

A Frost & Sullivan White Paper

INTRODUCTION

The benefits of a mobile-enabled workforce are undeniable and far-reaching. For business owners, increasing operational and business velocity is no longer tethered by time and place. The untethering benefits of mobility extend to employees, too, both in their personal productivity and in balancing their personal and work lives.

For IT, however, equitably facilitating workforce mobility across all of an organization's factions with each faction defining workforce mobility in its own terms is, to say the least, challenging. Too often IT is forced to make compromises. And with these compromises, one or more of the factions will be unsatisfied, potentially to the level that their dissatisfaction materializes in negative consequences elsewhere. Unfortunately, what was once considered an equitable compromise turns out to be a barrier in capturing the full benefits of workforce mobility.

Ultimately, technology can minimize compromises such that more or even all of the factions consider themselves winners. In this paper, we discuss why a bring-your-own-device (BYOD) approach to workforce mobility can be a compromise-free approach, and then how the combined capabilities of Samsung KNOX and Enterprise Mobility Management from AirWatch by VMware turn this compromise-free approach into reality.

THE FACTIONS AND THEIR WORKFORCE MOBILITY DEMANDS

One of the many benefits of today's technology era is technology democratization, that is, the widening range of technologies that are readily available to the general population. While technology democratization has been empowering for the individual in a consumerization of IT sense, where the individual can acquire and configure information technologies to his or her personal preferences, conflicts do arise. Typically, conflicts occur when the flexibility that the individual has grown to expect with consumerization of IT is at odds with the objectives of the community that includes the individual. Forced compromise, such as an individual subrogating some of his or her flexibility to accommodate the objectives of the community, usually and unfortunately follows.

Workforce mobility is a prime example of this conflict and compromise interplay. For instance, an individual's smartphone preference may be in conflict with the employer's data protection requirements. The resulting conflict-resolving compromise can materialized in many forms, such as narrowing employees' smartphone choices; provisioning locked-down, company-owned smartphones; or scaling back the hoped-for benefits of workforce mobility by restricting smartphone use in business operations to fewer employees. Any way the compromise is structured, one or more of the involved parties are relinquishing something that they desire.

Conflict and compromise do not have to occur in workforce mobility. The right set of technologies can reconcile conflicts without overt compromises. To arrive at this point, a comprehensive understanding of the preferences and objectives of each faction in the chain of workforce mobility is needed. Those factions include end users (employees and, depending on circumstances, contractors and business partners); business leaders, including those tasked with security and data protection oversight; and the IT organization. With a comprehensive understanding of preferences and objectives, a technology solution can be fitted into place. Following is our view on the workforce mobility preferences and objectives for these three factions.

Factions	***Workforce Mobility Preferences and Objectives***	
End Users ***(employees and select contractors, and business partners)***	**Convenience**	One device that can support both personal and professional needs, that is, supports dual personas or partitions within the same device.
	Self-Service	Device and application configuration must be intuitively self-serviceable because lacking this capability, end user adoption is stifled and IT helpdesk support could become strained (another deterrent to end-user satisfaction).
	Personality	Each end user can choose a mobile device that complements his or her personality (e.g., how the individual prefers to configure and use his or her device and the "statement" the individual wants to make, that is, under the notion that a mobile device is partially a fashion and status statement).
	Flexibility	The end user has complete decision authority on when to change devices and make the transition with no or little oversight or approval by others.
	Privacy	The end user's data and interactions are just that, the end user's and the end user's alone, and only viewable or accessible by those the end user directly authorizes.
	Protection	The end user's data, profile, configurations, and applications are also all and exclusively the end user's and unaffected by what happens in the professional partition. In other words, an iron curtain exists between the personal and business partitions.

Factions	Workforce Mobility Preferences and Objectives	
Business Leaders	**Employee Productivity**	Business leaders want maximum productivity from each mobile-enabled end user and from mobile-enabled workgroups. Consequently, the mobile device must be up to the business tasks demanded of it.
	Protection	Mobile devices, like PCs, are entry points into a business's IT resources (systems, applications, and files) and must have the same, if not more, controls over access and use of these resources. Similarly, mobile devices are file repositories and these repositories must be protected from theft, unsanctioned modification (i.e., file integrity), and misuse. Business applications running on the mobile device and the operating system must also be protected from compromise (e.g., malware) as compromises of the mobile device can propagate outward and contribute to business system compromises and data breaches.
	Low Exposure	Businesses that handle sensitive data (e.g., personally identifiable information—PII) are subject to the stipulations of data protection regulations and their audits, which can extend to BYOD devices. Therefore, these businesses need to efficiently and effectively manage their regulatory exposure pertaining to BYOD. Separately, access, whether originating from unintentional and benign acts or those that are malicious to the end user's personal information located in the BYOD device is unacceptable and potentially harmful to the business (e.g., a privacy violation). The BYOD solution or solutions should mitigate both of these exposures.
	Net Positive	Businesses expect a positive return in workforce mobility to ensure the cost of enabling workforce mobility and establishing and maintaining protections and controls does not exceed the benefits.
The IT Organization	**Certainty**	The workforce mobility approach must satisfy as many of the end-user and business leader preferences and objectives as possible.
	Scalability	The solution or solutions supporting a no-compromise outcome must easily scale with declining incremental costs as more mobile devices come under management. End-user self-service, as mentioned above, is a critical feature to both end users and the IT organization. Similarly, out-of-the-box and near-out-of-the-box integration with existing business systems, e.g., user directories, is also essential in contributing to seamless scalability.
	Adaptability	As new mobile devices are incorporated, the solution or solutions must support them automatically (i.e., very few to no workarounds required).
	Ease of Use	Specialized training to administer the workforce mobility solution or solutions is undesirable and adds to the already limitless tasks that IT organizations now face. Therefore, administration ease of use is critical.
	Customizable	Administrative access to manage different parts of the workforce mobility solution must be easily aligned with the structure of the IT organization and the business (e.g., tiered and role-based administrative access). This same capability is needed for creating and managing business-use policies and professional profiles of each end user.

WHY BYOD SHOULD BE THE DEFAULT APPROACH

This era of technology democratization and consumerization of IT has placed end users in the proverbial driver's seat pertaining to workforce mobility. Moreover, with the high penetration of personal smartphones, end users are equipped with the necessary equipment to at least attempt a portion of their business-related activities from their personal devices. Also, factoring in tablet adoption, faster 4G networks, and Wi-Fi availability, leveraging the convenience and familiarity of personally owned mobile devices in lieu of firing up corporate-issued laptops intensifies.

The Internet and consumerization of IT has also spawned an innate community of experimenters. The reasons are logical. For an increasing portion of end users, they grew up on the Internet. Their education was enriched by online resources, their multiple calendars were arranged and viewed over the Internet, and, of course, social media has altered behavioral norms. Collectively, this online upbringing has contributed to the viral sharing of links, apps and sites, and a "try first and ask questions later" instinct. In aggregate, the workers of today have the means and engrained behaviors to expand usage of their personally owned mobile devices, i.e., BYOD, into their professional lives.

For businesses contemplating a workforce mobility initiative, they should weigh the engrained behaviors of their employees and genuinely question whether a strategy that is not BYOD-first will succeed. If a BYOD approach is not pursued, consideration of the consequences of unsanctioned BYOD activity should be given. Those consequences run the gamut of data breach risk, uneven employee adoption of mobile business applications, and employee displeasure (work activities tethered to corporate-issued devices). Accordingly, a successful business initiative that involves its employees depends on their embrace of that initiative. If employee acceptance and adoption are low, meeting the objectives of a workforce mobility initiative will fail to meet expectations. Even so, a user-friendly, BYOD-first approach to workforce mobility does not guarantee a compromise-free reality or satisfying outcomes. Choosing solutions designed explicitly to meet the wide range of preferences and objectives of end users, businesses owners, and IT is essential; and is discussed next.

HOW SAMSUNG KNOX AND AIRWATCH MAKE COMPROMISE-FREE WORKFORCE MOBILITY A REALITY

The means to a compromise-free approach to workforce mobility is accomplished through the integration of capabilities from Samsung KNOX and AirWatch. The distinction between the two is one of a trusted platform (i.e., the foundation) as provided by Samsung KNOX and BYOD customization as provided by AirWatch. Each will be discussed in sequential sections.

Trusted Platform

Although containerization—the isolation of the business partition from the rest of the device—is an essential component in a BYOD approach to workforce mobility and supported by Samsung KNOX and AirWatch, building on a more secure and trusted platform comes first. Not unlike a building's foundation, the integrity of the business container and the certainty of the controls that can be applied to that container and its contents depend on the integrity of the platform. A foundation not designed and built to sustain the weight of the load placed upon it will eventually lead to building integrity issues; issues that are unlikely to be easily, if at all, shored up.

For Samsung KNOX mobile devices, integrity starts with its ARM® TrustZone® by linking a chain of trust from the boot loaders up through the container itself. In ARM TrustZone, reference values are etched into the Samsung KNOX hardware. During the device boot process, as the primary and then secondary boot loaders execute, values associated with each boot loader are compared to those etched into hardware. Matched values validate that the boot loaders have not been compromised and the boot loader processes continue to completion. A similar hardware-based value assessment is conducted for the next software layer, the Linux kernel. If the values do not match, loading of the kernel is terminated. Further adding to integrity assurance, the kernel and the next three software layers—SE for Android (OS), KNOX Framework, and ultimately the KNOX Container—are continuously monitored for the presence of compromises through the KNOX TrustZone-based Integrity Measurement Architecture (TIMA). Like the many steps of building inspection that occur during the construction of a commercial building and the periodic inspections of critical building functions (e.g., elevators, emergency lighting, and sprinkler system), Samsung KNOX ensures that a trusted platform is assembled and is sustained.

As a private room in a public space, the KNOX Workspace container is a virtual enclave on the mobile device for the hosting of business-sanctioned applications and data. Isolated from the rest of the mobile device, the "what's inside" this private room is IT-controllable. Although isolated from the rest of the device, the end user can still switch into and out of the container with single-click ease. However, because entering the container is easy for the end user, even imposters, Samsung KNOX devices support multi-factor authentication (MFA), such as an on-device fingerprint scan and PIN entry (i.e., something the end user is and something the end user knows). IT administrators can incorporate MFA into container user access policies.

To safeguard the container's data (i.e., data-at-rest) and to encapsulate communication sessions over public networks (i.e., data-in-motion), the enabling encryption keys are stored in hardware—another ARM TrustZone feature. Additionally, this same high degree of data-at-rest and data-in-motion protection can be extended to multiple containers on the same device and can be applied device-wide so that the end user's personal data and communications are equally protected. Being device-wide does not, however, nullify the iron-curtain separation between the professional and personal spaces. The end user retains privacy control over the non-containerized portion of the device.

In a world of constantly evolving technologies and products, business leaders and IT professionals are challenged to distinguish between genuine capabilities versus vendor assertions. Certifications help in this regard. Samsung KNOX has received internationally recognized security certifications from the Common Criteria (CC), National Information Assurance Partnership (NIAP), the National Institute of Standards and Technology (NIST), the Defense Information Systems Agency (DISA), and the Communications and Electronics Security Group (CESG). For additional information, see https://www.samsungknox.com/en/security-certifications.

BYOD Customization

Samsung KNOX establishes a trusted platform and protected enclave essential in the double-duty use of personally owned mobile devices in the business environment. While essential, Samsung KNOX is nevertheless incomplete in addressing every business's workforce mobility requirements and circumstances. At the same time, Samsung KNOX was not designed to meet this all-encompassing goal, particularly when AirWatch, an established Enterprise Mobility Management (EMM) solution provider, can leverage the security capabilities of Samsung KNOX to customize a BYOD-first approach to workforce mobility for each business.

Features of AirWatch demonstrate how BYOD can be customized. Those features include:

- **Multitenancy** – Just as logical and organizational workgroups within a business require unique sets of software applications and corporate system access privileges, the same is true for the containers in mobile devices. AirWatch supports an infinite number of policy groups for mobile containers, all from a single administrative console for devices with multiple containers and containers on different device platforms. In a workforce mobility environment of mixed platforms and device ownership models (employee-owned and corporate-owned), this AirWatch EMM feature assists IT organizations in aligning

policy with individual containers. For example, the policies for Samsung KNOX containers can be more expansive in end-user privileges and applications than policies for containers on mobile devices with platform integrity that is not as robust.

- **Role-Based Access** – A core security principle is least-access privilege. For IT system administrators, this means assigning access permissions based on an individual administrator's organizational role and security clearance (i.e., access limited to only what the role and clearance allows). AirWatch supports this feature, including the recording of administrator actions—an auditing necessity.

- **Terms of Use** – Even with the iron-curtain separation of containers on Samsung KNOX mobile devices from the rest of the device, instances of partial melding of the two personas are beneficial (e.g., business calendar entries viewable from the personal calendar and vice versa). With this melding, terms-of-use agreements need to be drafted, shared, and electronically signed so end users are informed of the business's rights and those rights are legally protected.

- **Security** – As summarized earlier, the security elements of Samsung KNOX mobile devices are purpose-built through a hardware-enabled design. AirWatch links into those capabilities so that administrators can create and enforce BYOD policies that balance security risk with end-user productivity, flexibility, and convenience (e.g., use a VPN on only a subset of containerized applications). Similarly, AirWatch's native security features (e.g., encryption) are extendable to non-Samsung KNOX devices.

- **Flexibility** – Unlimited policy groups and adaptive policy creation of AirWatch, as mentioned previously, affords AirWatch customers the flexibility they need to manage risk while enabling BYOD. For the end user, AirWatch supports all major mobile platforms and operating systems from day one in order to implement a flexible BYOD program. This allows employees to choose from the latest makes and models for their smartphones, tablets, and laptops without jeopardizing inclusion in their employer's BYOD program. AirWatch also offers IT-flexible deployment models. Customers can utilize AirWatch's cloud environment or install the software on premises in their own datacenters. As the IT policies change, customers can seamlessly migrate between AirWatch's cloud and on-premises environments.

- **Simplicity** – End-user self-service features are central to AirWatch. Through the AirWatch self-service portal, end users can enroll their devices, view device information, initiate actions (e.g., password reset), and request IT assistance. The benefits are twofold: (1) end users are served in a familiar and preferred do-it-yourself manner, and (2) the business saves money as fewer helpdesk resources are required and IT personnel can be redirected to focus on other business initiatives.

Stratecast

The Last Word

IT is placed in an inevitable position of referee in regards to workplace mobility. IT's two primary constituents, business leaders and their employees, have different perspectives on what they seek to gain from workforce mobility and how to get there. Business leaders, rightly so, want to maximize the benefits of a mobile workforce in driving business forward, but also want to accomplish this goal with minimal incremental costs and risks. Technology-empowered employees are mindful of business leaders' bottom-line proclivity, yet have their own perspectives on how workforce mobility should be accomplished. Central to their perspective is a healthy dose of flexibility in device selection and use, personal privacy, and to avoid the inconvenience and chaos of toting multiple mobile devices: one for business and another for personal use.

IT has experienced similar scenarios in the past as consumer technologies have entered the workplace. Web access, text messaging, inter-company email, and social media all started out as consumer-embraced technologies that seeped into the workplace by employees. IT, in many ways, was left holding the bag in reconciling this consumerization of IT with the business's risk-reward calculations. All too frequently, the initial response was to push back on consumerization of IT. This initial response was, as history has shown, eventually replaced with the embrace of these "new" technologies in the business. The process of going from fear to acceptance has, unfortunately, been littered with time- and resource-consuming starts and stops.

BYOD involving mobile devices can leapfrog the inefficiencies and errors of the past. As we described in this paper, a compromise-free approach to mobile BYOD is feasible. The combined solutions of Samsung KNOX and AirWatch can simultaneously support the demands of both business leaders and their employees without subrogating one for the other. Not to be overlooked, IT is not again left holding the bag, in this case cobbling together tools to support these two constituents. The tools and structure are present to assist IT in doing its job effectively and efficiently.

For businesses that have been on the fence in deciding how to facilitate workforce mobility or are dissatisfied with their current workforce mobility strategy, the timing is right for you to make a decision that produces a positive return. The combination of Samsung and AirWatch, as we described in this paper, is fully dialed into the collective needs and preferences of end users, business leaders, and IT to make a BYOD-first approach to workforce mobility satisfying for all. Additional information on their solutions can be found at www.samsung.com/knox and www.air-watch.com, respectively.

MICHAEL P. SUBY
Stratecast VP of Research
Frost & Sullivan
mike.suby@frost.com

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041