MARKET PERSPECTIVE

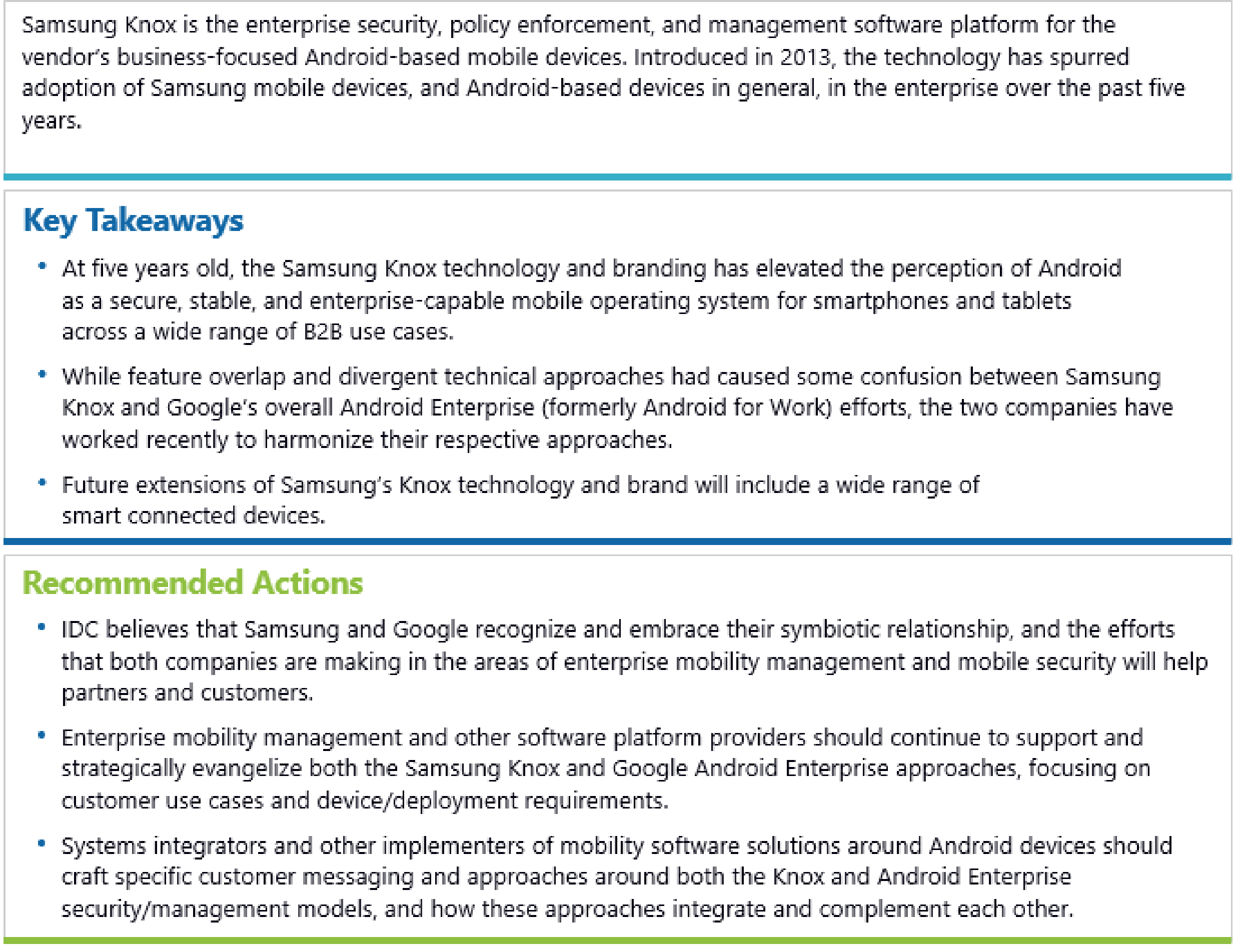
Samsung Knox at Five Years: Elevating Android's Enterprise Stature and Future Deployment Opportunities

Phil Hochmuth

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Samsung Knox Platform at Five Years — Key Takeaways and Recommendations



Samsung Knox is the enterprise security, policy enforcement, and management software platform for the vendor's business-focused Android-based mobile devices. Introduced in 2013, the technology has spurred adoption of Samsung mobile devices, and Android-based devices in general, in the enterprise over the past five years.

Key Takeaways

- At five years old, the Samsung Knox technology and branding has elevated the perception of Android as a secure, stable, and enterprise-capable mobile operating system for smartphones and tablets across a wide range of B2B use cases.
- While feature overlap and divergent technical approaches had caused some confusion between Samsung Knox and Google's overall Android Enterprise (formerly Android for Work) efforts, the two companies have worked recently to harmonize their respective approaches.
- Future extensions of Samsung's Knox technology and brand will include a wide range of smart connected devices.

Recommended Actions

- IDC believes that Samsung and Google recognize and embrace their symbiotic relationship, and the efforts that both companies are making in the areas of enterprise mobility management and mobile security will help partners and customers.
- Enterprise mobility management and other software platform providers should continue to support and strategically evangelize both the Samsung Knox and Google Android Enterprise approaches, focusing on customer use cases and device/deployment requirements.
- Systems integrators and other implementers of mobility software solutions around Android devices should craft specific customer messaging and approaches around both the Knox and Android Enterprise security/management models, and how these approaches integrate and complement each other.

Source: IDC, 2018

NEW MARKET DEVELOPMENTS AND DYNAMICS

Introduction

The IDC Market Perspective looks at the current state, and future, of Samsung's Knox mobile security software platform for enterprise devices, five years after the introduction of the technology in 2013. It is clear by various measures that Knox was a strong catalyst for Samsung and Android device growth in the enterprise over the past five years, as the platform introduced the core concepts of Android operating system (OS) hardening and other supporting services and features aimed at allying securing concerns regarding the open source mobile OS. Knox must evolve alongside Google's separate efforts to introduce enterprise-level security and manageability features to the Android ecosystem at large while maintaining feature differentiation for the Samsung Knox brand.

Industry Dynamics

How Samsung Knox Changed the Story Around Android Enterprise Security?

In 2013, Samsung introduced the concept of securing the Android operating system specifically for the enterprise and the B2B markets — a segment, at the time, that saw the declining dominance of BlackBerry and the ascending presence of Apple's iPhone as corporate-standard devices. The concept of BYOD and personal smartphones in the workplace emerged as a phenomenon, and IT departments were struggling to keep up with the rapid influx of powerful and cellular- and WiFi-connected devices entering the workplace.

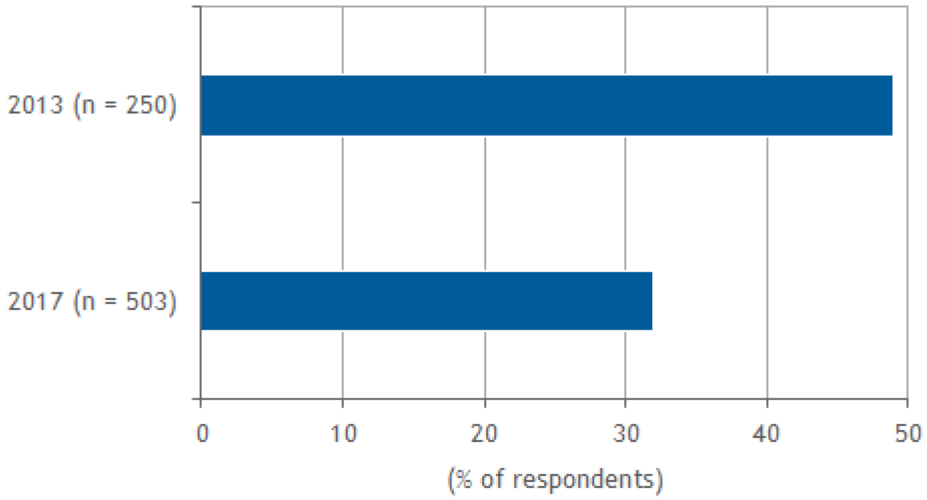
The first version of Knox was a part of Samsung's overall Samsung For Enterprise (SAFE) with Knox (now just branded Knox) effort. This introduced the concept of using a secure enclave, or a separate processing environment within the ARM process architecture, called the TrustZone, for embedding hardware and software security and authentication capabilities in the Android platform. BlackBerry devices had such capabilities for a while, but this was the first instance of this technology in the open source Android ecosystem at large scale. These capabilities were introduced with the Galaxy S4 and the Note 3. The initial launch of Knox also introduced the concept of the containerization to Android phones from a native device OEM perspective, allowing for work and personal apps and data to be segmented on devices. This app/data segmentation took advantage of underlying mandatory access control polices and permissions framework included in the underlying Android OS. At introduction, Knox also brought trusted/secure boot verification and remote attestation — or the ability to independently verify that a device is in a "trusted state" and was not tampered with or altered.

Knox emerged at a time when mobile security was in a bad state. According to IDC's 2013 *Enterprise Mobile Security Survey,* 59% of enterprises then said their organization had experienced a mobile malware incident or unwanted applications on corporate devices. Beyond just outright malware on devices, enterprises were beset with unknown devices and apps that were accessing corporate data with little visibility. Nearly half of the surveyed enterprises in 2013 said mobile data leaks were a major problem in their organization (compared with only a third of enterprises that cited this as an issue in IDC's most recent 2017 *Enterprise Mobility Decision Maker Survey*) (see Figure 2). The dual-personal approach of Knox, where personal (and potentially leaky) apps could be "sealed off" from corporate device environments, was appealing to businesses at the time it was introduced; according to the 2013 IDC survey, 72% of enterprise IT decision makers at the time said they wanted the dual-personality technology for work/private personnel on smartphones.

FIGURE 2

Mobile-Related Data Leaks, 2013 and 2017

Q. Has your organization experienced mobile-related data leaks?



Source: IDC's *U.S. Enterprise Mobile Security Survey,* 2013, and *U.S. Enterprise Mobility Decision Maker Survey,* 2017

Knox Iteration Reflects Maturing Enterprise Mobility Market

Subsequent iterations of Knox added more hardware- and software-based technologies such as enhanced key stores with enhanced Secure Element integration, real-time kernel protection and periodic kernel monitoring of the Android OS, fingerprint device access, SSL VPN support, and high-level compliant crypto (e.g., Federal Information Processing Standards [FIPS]). Subsequent advances in Knox versions 2.5 to 2.8 included malware scanning and more sophisticated utilization of key protection and sensitive processing (i.e., financial transactions). More sophisticated mobile VPN capabilities also evolved over this time (i.e., containerwide VPNs, per-app VPN, and VPN chaining). Client certificate management, split-billing support, enterprise-grade OTA firmware updates, and sensitive data protection were also introduced from version 2.5 to version 2.8 of Knox. Along this timeline, Knox started to overlap with the burgeoning Android for Work (AfW) capabilities that Google introduced in 2014 to improve and bolster security for all Android devices in ecosystem.

The emergence of Knox also coincided with the emergence and growth of the enterprise mobility management (EMM) market. In 2013, the market was still emerging, but on the verge of maturity; AirWatch, Good Technology, and Zenprise had yet to be purchased by VMware, BlackBerry, and Citrix, respectively, and MobileIron had not yet gone public. Microsoft had not yet introduced its EMM product Intune. However, enterprises realized they needed security and policy enforcement at the platform and device level, and this growing requirement is reflected in the 60% growth rate in the EMM market for 2013–2017.

Along the way, Samsung made key partnerships with over 15 enterprise mobility management and mobile device management solution providers to enable the activation and control of embedded Knox features. Much of the Knox feature set requires interoperability and the presence of an EMM platform to set and enforce the device-level polices and security capabilities Knox enables. Having as broad a support strategy as possible with EMM players was key for Samsung in getting Knox-enabled devices adopted and activated. The success of this strategy is reflected in strong growth in Knox activations over the past several years. Samsung estimates that more than 40 million enterprise mobile workers will use Knox in 2018, a number that has more than doubled year over year since 2013. Samsung forecasts that this same growth for Knox usage will continue through 2020.

The Knox Effect on Samsung and Android in Business Deployments

While Knox's release was a good for business Android uses, and the EMM industry, it helped buoy Samsung's device business as well. According to IDC's Worldwide Mobile Device Tracker, Knox and its subsequent iterations trace an overall steady growth trajectory of Samsung devices worldwide for 2013–2017. Samsung shipments increased at a compound annual growth rate (CAGR) of 15% over the same time period.

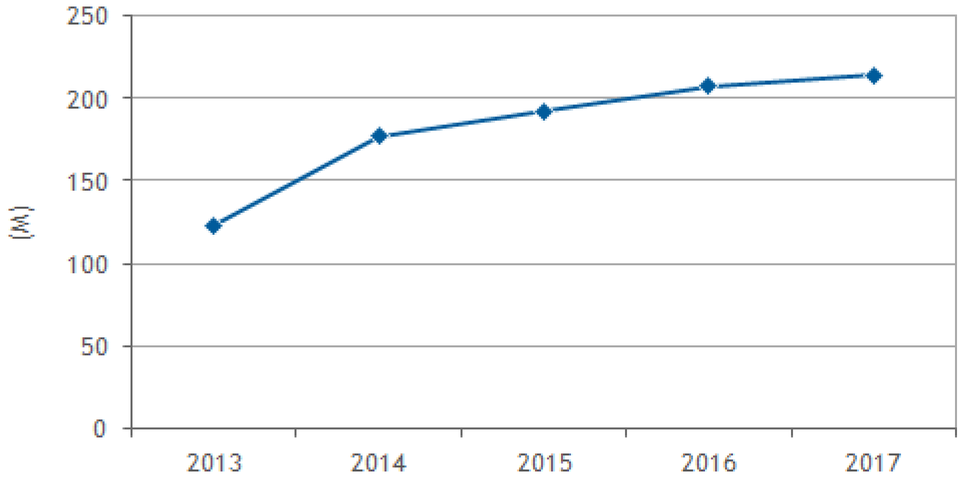
By introducing the idea that Android could be "made secure" and fit for enterprise use also spurred growth in business Android adoption. Google's Android for Work effort shortly followed the introduction of Knox and helped IT departments to allow more BYOD usage of the operating system.

Individual-liable (or BYOD) Android device shipments grew at a CAGR of 15% for 2013–2017 (see Figure 3). Concepts such as Knox and AfW also boosted Android as a corporate-issued smartphone standard, as corporate-liable or "commercial" Android devices grew 8% over the same time period.

According to IDC's business-use smartphone installed base data, Samsung, and Android in general, still has a way to go in terms of corporate acceptance, especially in the United States, where Apple is the predominant corporate-liable device brand deployed. However, the split between these two OSs has narrowed. Worldwide, the installed base of corporate-liable business-use Android devices has eclipsed that of Apple.

FIGURE 3

Employee-Liable Android Device Shipments, 2013-2017



Source: IDC, 2018

Knox and Android for Work Intersection/Evolution

While Knox and Android for Work promoted Android use in B2B deployments, the existence of these two standards also confused buyers about how to implement Android security and what features and technologies were supported in each approach. The feature gap between Android for Work and Knox has narrowed significantly over the past several years. Google rebranded Android for Work as Android Enterprise, the platform for OEM-agnostic Android security, management, and deployment, and made this capability a requirement for the Google Mobile Services (GMS) certification from device OEMs. This narrowing of features made it more difficult for businesses to discern the differences or value of one platform over another.

The feature overlap, and the bifurcated market approach to Android security among Google and Samsung, also made it harder for EMM partners to support customers looking into Android device deployments on their platforms. Management software partners struggled to support separate sets of code and API support to keep both Samsung and general Android device uses satisfied among their customer base. This caused some businesses to balk at Android investments and deployments among the customer base of many EMM vendors.

Harmonizing Android Security Efforts

The new approach in Android 3.0, dubbed as Knox + Android, emphasizes the fact that Android Enterprise is included inside the Knox platform with both features being available to users in parallel; the use of Android Enterprise feature does not preclude a Knox feature, and vice versa for Knox.

Samsung's goal is to reduce API support effort for EMM partners for Samsung and Google enterprise feature support and ultimately reduce confusion and complexity. Part of this effort involves changing the positioning of the Knox Workspace, a multilayered data separation capability with regard to the Android Enterprise profile available on devices across the OEM ecosystem. The goal was to standardize on areas where Knox and Android Enterprise overlapped, such as VPN management functionalities and data isolation. This new overall positioning is called Knox Platform for Enterprise.

Samsung still differentiates Knox features from Google's Android Enterprise with the Knox Platform for Enterprise offering – a paid premium offering for Samsung-supported devices, which goes further than the Android Enterprise feature set. Knox Platform for Enterprise provides enhanced features in the areas of certificate enrollment, advanced Microsoft Active Directory credential handling, more sophisticated VPN capabilities, audit logs, and government-grade security policy enforcements on devices. In all, there are more than a dozen additional security features available in the Knox Platform for Enterprise offering beyond the Android Enterprise feature set. The new solution also includes similar badging and icon for differentiating between personal apps and those protected by either the Android work profile or the Samsung work space on the Knox Platform for Enterprise.

Some parallel, and exclusive, features still exist between Android Enterprise and Samsung Knox, particularly in the area of deployment and enrollment. For example, Samsung Knox Mobile Enrollment (KME) is still the only preconfiguration capability for setting up and staging Samsung business devices for out-of-the-box enrollment into EMM platforms and other preset security and app configurations. Yet in late 2017, Google introduced the Android zero-touch enrollment technology as an Android Enterprise feature – a similar auto setup capability. Google is offering this to multiple Android device OEMs; however, Samsung chose not to adopt this as a supported partner in this technology to avoid confusion with customers.

The Google Enterprise Recommended program, launched in the first quarter of 2018, is another Android-focused initiative that provides a baseline set of support for enterprise features required from device OEM partners and carriers. Google's intent with Enterprise Recommended is to spread the same level of enterprise-grade feature support (and customer assurance) to a wider audience of OEM partners and device makers. While Samsung chose not to participate in Enterprise Recommended, many of the requirements of the program are specific features and capabilities that have been present in Knox for the past several years.

What's Next for Samsung, Enterprise Android, and Knox

Beyond the smartphone, Samsung has ambitious plans for the Knox architecture, platform, and brand. While very different technically, Knox will be extended to platforms such as Tizen, which runs on Samsung wearables and other smaller devices. Samsung says that many other connected electronics and products the company makes (smart TVs, consumer appliances, IoT devices, etc.) will adopt the Knox brand and its core concepts — OS kernel hardening, attack surface reduction, active vulnerability scanning, hardware-assisted crypto, and a key store — either in parts or overall, where applicable. From an enterprise perspective, this will be critical in areas such as wearables and AR/VR; industrial use cases such as medical, military, law enforcement, and sensitive manufacturing deployments will require high levels of device control, policy enforcement, and data security, which are all in the Knox wheelhouse.

ADVICE FOR THE TECHNOLOGY SUPPLIERS

EMM vendors should embrace and support both the Samsung's Knox Platform for Enterprise and Google's Android Enterprise/Enterprise Recommended programs to ensure their management platforms can address the largest number of use cases and deployment scenarios for Android devices. Consolidated API support and clear delineation between feature sets will make this easier and expand the possibilities for Android deployments among customers. This will help EMMs and partners support the wide set of Android deployment scenarios. For example, some customers may look specifically for Samsung devices, or with high-security requirements addressed by Knox Platform for Enterprise. Other customers might require lower-cost Android devices from other OEM providers or support for alternative Android brand preferences in specific regions; Android Enterprise and Android Recommended can help support these instances.

IDC'S POINT OF VIEW

IDC believes that Samsung and Google recognize and embrace their symbiotic relationship and that the efforts both companies are making in the areas of enterprise mobility management and mobile security will help partners and customers. In terms of enterprise feature sets and security advancements, Knox (and its future iterations) and Android Enterprise are both good for enterprises in the long run.

LEARN MORE

Related Research

- *Worldwide Enterprise Mobility Management Software Market Shares, 2017: Evolving Mobility Use Cases Drive Market Growth* (IDC #US43293918, May 2018)
- *Worldwide Business Use Smartphone Forecast, 2018-2022* (IDC #US43634018, March 2018)
- *Samsung Reimagines Camera and Enterprise for Galaxy S9 at MWC 2018* (IDC #lcUS43591018, February 2018)
- *Worldwide Mobile Enterprise Security Software Forecast, 2017-2021* (IDC #US43311217, December 2017)

Synopsis

This IDC Market Perspective looks at the current state, and future, of Samsung's Knox mobile security software platform for enterprise devices, five years after the introduction of the technology in 2013.

"Going on five years, Samsung's Knox platform has created strong value for enterprises deploying Android-based smartphone and tablet technologies across a wide range of use cases," says Phil Hochmuth, program director, Enterprise Mobility at IDC. "The future of secure Android deployments in the enterprise is strong as Samsung and Google continue to refine their respective approaches to supporting business deployments of the open source mobile OS at scale.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.