PIQUE SOLUTIONS

Windows 10 versus Samsung KNOX 2.4.1

An Addendum to the Windows 10 versus Android 6 White Paper: Analysis of Samsung KNOX 2.4.1 in Security and Manageability Categories

PIQUE SOLUTIONS

July 2016

MICROSOFT SPONSORED THE DEVELOPMENT OF THIS WHITE PAPER. THE UNDERLYING LAB TESTING AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | www.piquesolutions.com

Contents

Executive Summary

In addition to the analysis of Windows 10 vs. Android 6 with Android for Work, Pique Solutions conducted a lab-based analysis of Samsung's KNOX 2.4.1. This analysis looked at the same capabilities for resilience to assess the level of assurance KNOX provides and the impact on usability that resulted from implementing those capabilities. Because KNOX is a secure container layered on top of Android, the analysis focuses on what new enhancements it provides and how those affect the previous assessment of Windows 10. This paper is not a complete analysis of the Android OS or Windows 10; that analysis can be found here: Windows 10 vs. Android 6 Security and Management Comparison White Paper.

With Windows 10 and Windows 10 Mobile, Microsoft has unified the PC, tablet, and phone operating systems into a single OS. Windows 10 and Windows 10 Mobile are co-developed, share the same core and the same app model, and access the same app store. As with our research on the Android paper, we looked at Windows 10 Pro, Windows 10 Enterprise, Windows 10 Mobile, and Windows 10 Mobile Enterprise. In some cases, the underlying chipset allows for extra functionality, such as virtualization support on x86 processors, or the OS version has specific features related to its core function, such as telephony on Windows Mobile. Otherwise, security, management, and apps built on the Universal Windows Platform are the same across PCs, tablets, and mobile devices. This paper will refer to the operating system as Windows 10, with variances and differences noted where applicable.

The latest version of KNOX is 2.6, released in February 2016, with support for Android 6. Although this version is on the roadmap, it is not available for the device Pique tested—a Samsung Galaxy S6 Edge on AT&T. This was the latest device available from Samsung up to the recently released S7. The latest build available from AT&T is Android 5.1 with KNOX 2.4.1. More importantly, Samsung notes the Samsung Galaxy S6 Edge will only receive KNOX 2.5. This version fragmentation is quite common with Samsung devices and software, with even the flagship devices behind on Android updates by as much as 6 months.

KNOX does provide enhanced functionality on select Samsung Android devices, and it provides Android 6 with Android for Work a greater degree of security assurance within its secure container. KNOX introduces some key features lacking in Android for Work, specifically two-factor authentication for Active Directory (AD) authentication, hardware root-of-trust remote attestation, and a streamlined provisioning process.

Overall, the container approach is still limited in relation to the Windows 10 approach, which provides its functionality at the device and data levels. Even though Samsung KNOX measurably improves on Android security, it is not a comprehensive security solution for organizations with Android devices from multiple manufacturers. The biggest limitation is Samsung is a hardware manufacturer at its core, not a software company, as is reflected in its earnings. Samsung develops new hardware rapidly, and often new versions of software, including KNOX, are becoming hardware-dependent. This rapid hardware update cycle creates fragmentation within Samsung's own enterprise software environment. To the enterprise, this could mean constant hardware refresh cycles or opting out of access to new functionality in what is still a rapidly developing market.

In short, both from our testing and from our overall analysis of the mobile OS market, we find Windows 10 still maintains a higher level of assurance and less of an impact on usability. KNOX mimics many of the features that Windows 10 incorporates at the OS level, and in some areas KNOX has deep hooks into Android, but it is still an additional layer of software. In this white paper, we will describe the differences between the two platforms and the features and capabilities that led us to this conclusion.

Testing Methodology

Pique leveraged previous research for Android 6 and Windows 10 for this assessment. For KNOX, the steps were as follows:

1. Leverage existing data from Android 6 and Windows 10 testing.
2. Identify those areas where KNOX enhances Android 6.
3. Test functional areas specific to the secure container and KNOX enhancements.
4. Manually confirm how the Samsung Android device performs in the selected tasks.
5. Publish an assessment of the findings.

To assess Windows 10 and Android 6 with Samsung KNOX using industry-accepted standards and definitions, Pique Solutions referenced the security characteristics and required capabilities founded in the principles identified in Special Publication (SP) 1800-4b of the *National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide.* The NIST analyzed the content and concepts from multiple standards to generate the necessary security characteristics, including findings documented in NIST SP 800-124, NIST SP 800-164, the National Security Agency (NSA) mobile capabilities package, and the appropriate National Information Assurance Partnership (NIAP) protection profiles. Pique Solutions revised and updated the NIST characteristics where it deemed appropriate to address missing functionality, to correlate security characteristics with vendor-described capabilities, and to improve the overall presentation and flow of the paper.

We grouped the capabilities into four areas.

Identity and Authorization

- Authentication: Local authentication of user to device and apps, remote authentication of user, remote authentication of device
- Trust Model: Implementation of user and device roles for authentication, credential and token storage and use
- Biometric Support: Methods, store, use

Information Protection

- Protected Storage (Data at Rest): Device encryption, trusted key storage, hardware security modules
- Protected Communication (Data in Transit): Virtual private network (VPN), per-app VPN
- Data Protection in Progress (Data in Use): Protected execution environments, data management, data sharing

Threat Resistance

- Device Integrity: Boot, OS, app, and policy verification; trusted integrity reports
- Application Protection: Memory isolation, trusted execution, browser protection

Management

- Device Enrollment: Discovery, certificate, provisioning
- Device Configuration and Policies Supported: Network, device resources management, geo-fencing
- App Management: Delivery, update, configuration, app black-/whitelisting
- Remote Assistance: Asset management, OS and security updates, lost device, remote wipe

- Monitoring: Anomalous behavior detection, compliance, root detection

For the testing environment, we used Microsoft Windows Server, Microsoft Active Directory, Office 365 (documents and email), "Enterprise App" (a lightweight limited-functionality app to simulate an enterprise provided app), "Personal App" (a lightweight limited-functionality app to simulate a personal app), and OneDrive. The mobile device management (MDM) system used was MobileIron.

The devices used were the following:

a. Lumia 950—Windows 10 Mobile
b. Surface Pro 3—Windows 10 Enterprise
c. Samsung Galaxy S6 Edge—Android 5.1 and KNOX 2.4.1
d. Samsung Galaxy Note Edge—Android 5.1 and KNOX 2.4

For the purpose of parity, Pique Solutions chose MobileIron to be representative of a third-party MDM tool commonly present in the enterprise. Identifying and reviewing functionality of MDM is beyond the scope and intent of this paper.

To assess OS resilience, we analyzed security and management capabilities against security assurance levels (SALs), a concept introduced in ISA-99.01.01**.** ISA99 qualitatively defines four SALs:

- SAL1—protection against casual or coincidental violation
- SAL2—protection against intentional violation using simple means
- SAL3—protection against intentional violation using sophisticated means
- SAL4—protection against intentional violation using sophisticated means with extended resources

For scoring, SALs are assigned numerical values and weighted on utility of capabilities to organizational security. Utility defines whether or not a capability provides features an organization needs. The total score reflects an overall OS resilience level, or how well an OS would survive an attack and to what level. Pique also evaluated the impact security had on usability. Metrics are time-to-task, error rate, and user satisfaction. Information security always fails to human error when it provides a poor user experience.

Key Findings

Based on Pique Solutions' lab-based comparative feature assessment of Windows 10 and KNOX 2.4 in the security and manageability categories, Windows 10 provides a better option than KNOX 2.4 for the enterprise. The particular factors that led us to that conclusion are the following.

Identity and Authorization

- Windows 10 is the first major OS with Fast ID Online (FIDO) 2.0 support for the enterprise.
- KNOX Workspace supports AD-based two-factor authentication.
- Windows 10 biometrics eliminates passwords to improve both security and usability.
- Samsung has adopted the Android 6 fingerprint APIs on new devices, but it still needs work on older legacy devices; the Android fingerprint API is not supported on KNOX 2.4.

Information Protection

- Windows Information Protection (WIP) manages business data transparently with no impact to usability incurred from secure containers and app wrapping.

- Samsung KNOX data controls apply to KNOX Workspace, but these are limited to those apps in the container and require an all or nothing data-sharing approach.

Threat Resistance

- Windows 10 Measured Boot uses hardware to measure the system boot process for integrity.
- Samsung KNOX ensures Android has hardware root of trust laid down during chip fabrication.
- Windows 10 has strong memory controls coupled with extensive integrity validation.
- Samsung KNOX enhances Android memory protection with real-time kernel monitoring of apps in the secure container.

Management

- Samsung KNOX provides remote health attestation to report on device integrity before allowing access to its secure container, however it is not as dynamic as Windows 10.
- Microsoft delivers OS and security updates on an ongoing basis to Windows 10 directly from Windows Update.
- Samsung KNOX leverages the Google Store and update process for hardware and OS updates.
- Samsung has a poor history of updating devices in a timely manner; many devices are never updated, as they are dependent on carrier support and Samsung moves on to newer hardware.
- Microsoft provides updates for all devices running Windows 10 on all carriers.

Testing Scores

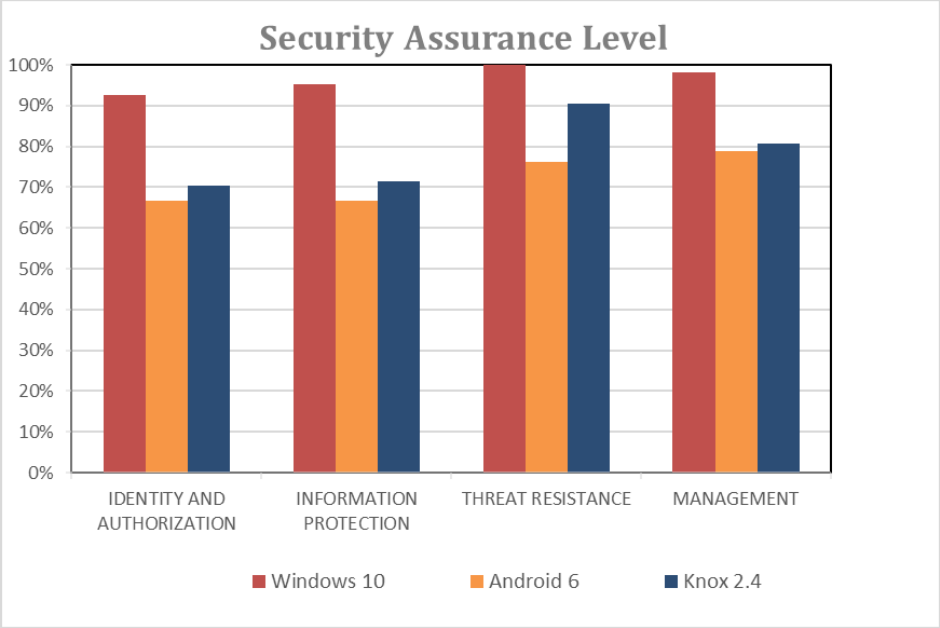

Chart 1. Windows 10 vs. Android 6.0 vs. Samsung KNOX *Security Assurance* Lab-Testing Scores

KNOX 2.4.1 provides incremental improvements in SLAs for Android, but it does not significantly shift the balance in any meaningful way. We can see the largest improvement occurs with Threat Resistance, as KNOX 2.4.1 introduces new memory protection techniques. More significant would be hardware root-of-trust remote attestation abilities. Remote attestation using hardware integrity checking is one the most significant new techniques for providing resilience to systems. It provides continual awareness

of system health while proving highly difficult to evade. It is a critical feature of resilient systems. An area where we would like to see significant improvement, and where Windows 10 still maintains a strong advantage, is with frequency of OS and security updates. The short software support life cycle for Samsung devices contradicts the long-term service requirements expected of most enterprises, in particular for maintaining policies consistent across old and new devices. For usability, in some ways KNOX improves Android, as with native two-factor domain accounts, but in others it has no impact. Two-factor domain authentication is nice, but only to the container, so it does nothing for device provisioning (unless you treat the container as the device) or local authentication.

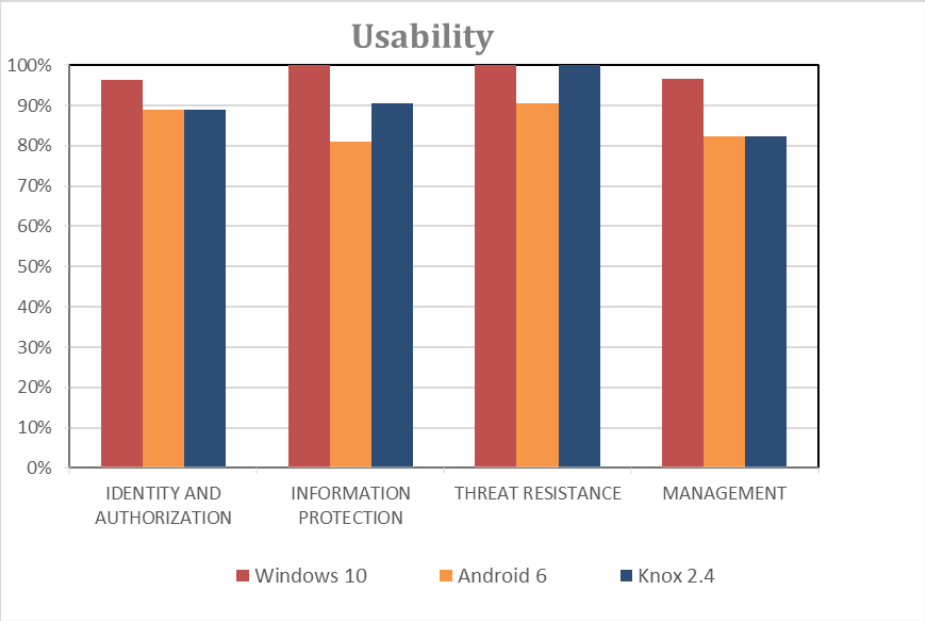

Chart 2. Windows 10 vs. Android 6.0 vs. Samsung KNOX *Usability* Lab-Testing Scores

Identity and Authorization

Identify and Access Management (IAM) provides all the appropriate resources to those users who need them when they need them. IAM should ensure integrity and authenticity of each user's identity while considering costs of the IAM infrastructure. More importantly, IAM must maintain user simplicity balanced with strong authentication controls.

Authentication

Windows 10 supports two-factor authentication for remote authentication of a user to a device and apps. Windows Hello technology replaces passwords with the combination of a specific device and a biometric gesture or PIN. Windows Hello supports Microsoft accounts, Active Directory, Azure AD, or a non-Microsoft service that supports FIDO 2.0 authentication. Windows 10 is the first OS to utilize FIDO 2.0 in an enterprise environment, and it is a major step forward. FIDO 2.0 supports multifactor authentication with asymmetrical keys in conjunction with hardware-based attestation to confirm the legitimacy of the keys.

Samsung KNOX supports two-factor authentication as the unlock method for the KNOX secure container using a combination of fingerprint and password, PIN, or pattern. KNOX provides an option to use an AD password as the unlock method for KNOX containers. Additionally, single sign-on is available for services inside Workspace. The user on the mobile device can change AD passwords from the Settings menu inside the KNOX Workspace container. When configuring single sign-on, the password

change does not require entering the password a second time. KNOX Workspace makes use of ARM TrustZone–based components together with the user's credentials to protect cryptographic material and strengthen the protection of data contained within it. While secure, ARM TrustZone is part of the system on chip architecture and uses shared system resources for storing cryptographic information. Samsung KNOX does not require the use of a Google email account.

Biometric Support

The Windows Hello framework offers strong two factor authentication with biometrics that helps protect corporate identities and minimizes the need for or use of passwords. The Windows Hello companion device framework enable the use of a Windows 10 phone to unlock a Windows 10 PC, or other companion devices to unlock a Windows 10 Mobile device. Windows Hello supports fingerprints, facial recognition, and iris scanning, with the ability to support other forms of biometrics in the future.

KNOX 2.4 leverages the Samsung API for fingerprint reading, allowing a user to use a fingerprint to unlock a device and the KNOX container. KNOX 2.6 will use the Android 6 fingerprint API for authentication and other tasks. Fingerprint matching occurs in a Trusted Execution Environment (TEE), which includes having all identifiable fingerprint data encrypted and cryptographically authenticated within the TEE.

Testing Scores

Identity	SAL	Usability
Windows 10	**89**	**93**
KNOX 2.4	**70**	**89**

Here we see little improvement in security assurance on Android with the addition of KNOX 2.4.1. Why? The reason is simple. Because KNOX is a secure container running on Android 5.1, it does nothing for local authentication to device or local apps and, more importantly, Google has made significant improvements with Android 6 that KNOX users have yet to benefit from. For example, KNOX 2.4.1 does not have access to the Android fingerprint API only available in Android 6, limiting the value of the Samsung fingerprint authentication. It did not provide the best user experience and it is not as integrated in the system as on the Nexus 5X running Android 6, which provided a better user experience.

Information Protection

As defined in data loss prevention, data controls relate to three functional groupings that adhere to the data life cycle. These are data at rest (DAR), data in transit (DIT), and data in use (DIU). In any data protection strategy, controls would be located as close to the data as possible. This means the most effective method for data protection would implement controls on the data itself, followed by the apps that often serve as data custodians, followed by those on the device and then on the network. Often controls will exist at all of the above locations for complete management of the data life cycle.

Protected Storage (DAR)

The objective of controls for DAR is to ensure a lost, stolen, or misused device does not lead to the loss or compromise of sensitive information. Windows 10 implements device encryption, based on BitLocker technology for whole disk encryption, including operating system and data storage partitions. Windows 10 applies encryption automatically when policy requires it or the user enables it in the Windows settings. Windows 10 accelerates encryption through processor extensions to avoid compromising device performance. The default encryption algorithm is 128-bit AES.

KNOX bounds Android's kernel-level full-device encryption key to trusted hardware. KNOX Workspace encrypts all data generated from within the container and residing in storage. The decryption key for encrypted data is stored encrypted by the device-unique hardware key (DUHK). The default encryption algorithm is 256-bit AES. Additionally, KNOX provides Sensitive Data Protection (SDP) to encrypt data in a locked Workspace. The key used to encrypt sensitive data on disk is recoverable only if the user enters the Workspace password, PIN, or pattern or by a remote admin. After locking Workspace, SDP clears all keys in memory. SDP also flushes sensitive file data from the OS kernel's disk caches if the file is not in use by a Workspace application. Currently, email subject lines, body text, and attachments are marked sensitive. Additionally, the SDP Chamber provides a directory where all files are automatically marked as sensitive and are protected by SDP. Managed Profile apps have SDP enabled by default.

Protected Communication (DIT)

The objective of controls for DIT is the ability for the user to establish a protected connection between the device and trusted enterprise resources or with enterprise apps. Windows 10 supports a number of OnDemand and Enforcement methods to simplify and secure the VPN connection. Always On enables the VPN to connect automatically when the user turns on his or her phone or if there is a network change. LockDown VPN further enforces policy by only allowing network traffic over the VPN tunnel. App-triggered VPN allows for automatically triggered connections when an app launches. Traffic Filters offer enterprises the ability to manage per-app behavior so that only traffic originating from an approved list of apps flows across the VPN. As another layer, Traffic Filters also provide traffic filtering based on host destination attributes. Rules can include both app-based and traffic-based.

In addition to the default Android options, KNOX enables additional modes of granular VPN capabilities for both Workspace and the individual apps. KNOX VPN supports multiple concurrent VPN connections allowing for IPsec or SSL VPNs with configurable auto-reconnect and VPN tunnel chaining. KNOX VPN includes administrator-configured System VPN, Per-App VPN, and Workspace VPN. KNOX supports multiple concurrent VPN connections, including support for the standard Android IPsec, SSL, and common access card–based authentication. KNOX supports Always On VPN connections with auto-reconnect to the KNOX secure container. The KNOX VPN subsystem also supports other forms of packet processing, including split billing and network access control.

Data Protection in Progress (DIU)

The goal of data protection in progress is to limit the sharing of enterprise data with personal apps and services to prevent data leaks. Windows 10 WIP does not require the implementation of a secure container or duplicate apps for separating personal and enterprise data. WIP will be able to classify data as personal or business related and which apps are trusted or not trusted. This classification determines which apps will have access to business data, what data to encrypt, and how users can share that data. Windows 10 apps designed to work on personal and business data in parallel apply business rules to specific data to prevent leaking. AppLocker manages app classification sans app wrapping or any app modification that requires integrating with an SDK. This means admins do not need to add or remove

any classified app from a device, including when wiping enterprise information. WIP-aware apps do not tamper with existing personal apps and data.

KNOX Workspace provides an isolated environment and UI for enterprise use, consisting of a separate home screen, launcher, enterprise apps, and widgets. KNOX protects data owned by apps in KNOX Workspace. KNOX policies regulate sharing of information between Workspace and personal apps. This includes sharing of calendar, contacts, and notifications. The Workspace environment blocks copy/paste clipboard data from the personal environment, and vice versa. The same set of capabilities are present in Android for Work on Android 6. With KNOX 2.0, app wrapping was no longer a requirement. However, as with Android for Work on Android 6, a user must still download a separate version of any app that is going to run in the KNOX container, resulting in a more cumbersome user experience.

Testing Scores

Information Protection	SAL	Usability
Windows 10	**95**	**100**
KNOX 2.4	**71**	**90**

As with Android 6, we did not observe any particular advantages or disadvantages to device encryption or VPN communication implemented in Windows 10 and KNOX 2.4.1. These are strong for both platforms. What we do see again is that KNOX 2.4.1 provides only incremental upgrades to Android 6, which leverages its own secure container in Android for Work that provides similar data management controls and app resource utilization. Android 6 also implements TEE for hardware-based key management. The gains in usability come from better implementation of hardware cryptography and some improvements in data management controls, but still to the container.

Yet, as was identified when comparing to Android 6, Windows 10 still shows higher levels of assurance when managing business data given the granular level of encryption to data versus applying encryption and data controls to the container. WIP is transparent to most users, who might not know it is there until they attempt to perform an unapproved action and receive a notification.

Threat Resistance

To reduce the impact of data loss and malware propagation on a compromised system, operating systems need to be resilient. They need to be designed in a manner that prevents new or unknown apps from gaining reasonably broad or complete access to files stored on the disk or apps running on the device.

Device Integrity

Windows 10 devices utilize the Unified Extensible Firmware Interface with Trusted Boot to validate the integrity of the device, firmware, and bootloader using cryptographically validated digital signatures. This process establishes an essential root in a chain of trust that extends from the device hardware and firmware to the OS. After the OS loader starts, Trusted Boot verifies that the remaining Windows boot-related components are trustworthy and have integrity. The Windows kernel, in turn, verifies every

other component of the Windows startup process, including the boot drivers and startup files. Trusted Boot will detect any file modifications and attempt to restore those files to a known valid configuration before starting Windows.

Microsoft extends the primary integrity validation process by including a second hardware-backed process called Measured Boot. This uses TPM hardware to baseline the boot process for critical startup-related components, including firmware, Windows boot components, and drivers. TPM provides isolation and protection of the baseline data against tampering attacks. Windows 10 can leverage this baseline data along with additional security and configuration criteria for Conditional Access scenarios that will leverage the Windows Device Health Attestation (DHA) cloud-based service as a means to attest remotely that the device truly has integrity. From here management systems using the DHA service may grant or deny the device access to resources based on this check. This is particularly important in detecting rooted devices that may be able to circumvent less sophisticated integrity controls.

KNOX incorporates a number of system protection mechanisms in addition to Android. KNOX security begins with the device root key (DRK), a device-unique asymmetric key burned into the hardware at time of manufacture and signed by a Samsung certificate that confirms Samsung produced the DRK. The DRK is only accessible by specially privileged software modules within TrustZone Secure World.

KNOX Trusted Boot requires each software component to measure and stores the cryptographic hash of the next component in the TrustZone Secure World memory before loading it. If the signature verification fails, KNOX records the tampering by tripping a one-time fuse, called the KNOX Warranty Bit. This fuse identifies whether or not the device has ever booted in an unapproved state. If the Trusted Boot process detects that unapproved components are used, or if certain critical security features such as Security Enhancements for Android are disabled, it trips the fuse. If Trusted Boot trips the fuse, the device cannot run Android for Work, the device revokes access to the DUHK and the DRK in TrustZone Secure World, and the user cannot recover enterprise data on the device. For health attestation, stored measurements allow a third party to identify software versions to verify that the system only runs the latest versions, complementing the Rollback Prevention feature that prevents downgrading of patched software to an earlier version.

To prevent unauthorized modifications to the system partition, KNOX integrates a customized implementation of DM-Verity, a Linux/Android kernel module that performs integrity checks on all data blocks. In the basic Android implementation, DM-Verity uses a hash tree to perform integrity checks of individual data blocks; an RSA key signs the root of that hash tree. When a data block is read into memory, DM-Verity computes the hash of the block, and uses it, along with the other hashes on the path to the root to compute the root hash. If the result matches the signed version, the block is considered good. If not, access to the data block is restricted. The KNOX implementation of DM-Verity differs from the basic Android implementation in supporting file-based firmware over-the-air (FOTA) software updates, which is easier to support with the existing infrastructure.

Application Protection

Windows 10 apps and even portions of the OS itself run inside their own isolated sandbox called AppContainer. Windows 10 makes address space layout randomization (ASLR) available for apps while it applies ASLR holistically across the OS to help mitigate the risks of sandbox escapes. Windows 10 implements Data Execution Prevention to refuse to execute any code located in user-writable areas of memory, protected random heap memory allocations, and memory-management algorithms. This

collection of technologies further reduces the likelihood that vulnerabilities can enable successful exploits. To counter these defense mechanisms, attackers leverage code that is already available on the system, using return-oriented programming. Windows 10 is the first OS to implement a method for enforcing the flow between memory allocation and apps, dubbed Control Flow Guard (CFG). CFG verifies that the code location called is trusted for execution. If CFG does not trust the location, it immediately terminates the app as a potential security risk. This is critical for browsers, and Microsoft Edge is CFG-enabled. These groupings of technologies represent Microsoft's decades of experience combatting malware on Windows platforms, which have been the most used OSs by both enterprises and consumers.

In addition to Android app container access controls, KNOX includes a real-time kernel protection (RKP) feature—a memory security monitor located within an isolated execution environment. This environment is either Secure World of ARM TrustZone or a thin hypervisor protected by hardware virtualization extensions. RKP takes full control over memory management and intercepts critical events to inspect their impact before execution. RKP prevents a device from running code that does not have kernel privileges by preventing modification of kernel code and blocking injection of unauthorized code into the kernel or execution of user space code in privileged mode. RKP prevents user processes from directly accessing kernel data, including preventing double mapping of physical memory that contains critical kernel data into user space virtual memory. RKP protects the data that defines credentials assigned to running user processes to prevent attacker credential escalation.

Testing Scores

Threat Resistance	SAL	Usability
Windows 10	**100**	**100**
KNOX 2.4	**90**	**100**

This is the first and only area where we observed not just appreciable gains in KNOX 2.4.1 over Android 6 but also where KNOX 2.4.1 begins to achieve parity with Windows 10. They have similar capabilities for threat resistance. What is most significant is the observed impact of what a hardware root-of-trust with remote attestation capabilities has on the overall resilience of a system. This is one of the most innovative and perhaps important features to combat advanced threats. It is a strong characteristic of resilience and immediately provides higher levels of assurance when implemented. This functionality alone would make KNOX 2.4.1 a worthwhile improvement over Android 6. Windows 10 not only has the same capability, but also boasts a broader implementation that is system-wide and leverages dedicated hardware with the TPM chip.

Management and Reporting

Device management should optimize the functionality and security of a mobile infrastructure while minimizing cost and downtime. Device management provides four key capabilities: visibility, device configuration, app management, and operational support. Device management needs to consider organizations will allow the use of personal devices for access to corporate resources, corporate-owned devices only, or a combination of the two.

Device Enrollment

The current versions of management tools manage all device types running Windows 10. Existing enterprise management tools, such as Group Policy, Windows Management Instrumentation, PowerShell scripts, Orchestrator runbooks, and System Center tools, will continue to work for Windows 10 on PCs. Devices running Windows 10 also include a built-in MDM agent to enroll and manage devices. MDM vendors use the Microsoft MDM protocol for communication with a Windows 10 device, which supports Open Mobile Alliance's Device Management Protocol 1.2.1. The MDM client allows MDM to configure policy settings, deploy apps and updates, and perform other management tasks. MDM sends configuration requests and collects inventory through the MDM client.

KNOX classifies management policy groups into two major categories: Standard and Premium. Samsung developed the Standard Policy over the Google Android management capability beginning in 2009, and it is available to MDM vendors free of charge. The KNOX Premium Policy suite includes the policy groups offering and advanced capabilities such as management and control of KNOX Workspace, security features such as the Trusted Boot–based TIMA Keystore and Client Certificate Manager, Per-application VPN, and others. The SDK for these policy APIs is available at no charge; however, use of these features requires the purchase of a KNOX license.

Table 1. Windows 10 vs. Samsung KNOX MDM Support

	Windows 10	KNOX*
Absolute Software		√
BlackBerry	√	√
Citrix	√	√
Google		
IBM (MAAS360)	√	√
Lightspeed Systems	√	
MarkAny		√
Matrix 42	√	
Microsoft Intune	√**	
MobileIron	√	√
Nexdigm		√
NQ Mobile		√
SAP	√	√
Sophos		√
Soti	√	√
Symantec	√	
VMWare AirWatch	√	√

***** Each supports a different subset of KNOX features.
** Support for Android for Work will soon be added to Microsoft Intune.

Windows 10 personal-owned devices use a Microsoft Work Account, which acts as a secondary account on the device specific to enterprise management and resource access. Corporate-owned devices join the enterprise using domain accounts as the primary device authentication. Azure AD integration allows for single sign-on to native applications such as Mail, Word, and OneDrive; Azure AD web apps; on-premise resources; and Windows Store for Business.

Android requires the user to download an agent app from the Google Play Store. KNOX simplifies the enrollment process by either self-discovery using an email domain, or the IT administrator provides employees an enrollment link sent via email, text message, or the company's website, where they enter

their corporate email address and accept all required privacy policies and agreements. Users then enter their corporate account password for authentication, and KNOX automatically downloads and installs an agent. KNOX Mobile Enrollment also supports cloud-based device configuration for automatic staging and enrollment.

App Management

Windows 10 supports integration of Windows Store for Business subscriptions with MDM to deploy apps. To use an MDM system to deploy line-of-business apps directly to devices, a certificate authority must cryptographically sign software packages. An enterprise can deploy a maximum of 20 self-signed line-of-business apps to a Windows 10 Mobile device and more than 20 if the organization's devices run Windows 10 Mobile Enterprise. Windows 10 AppLocker for WIP specifies which apps are allowed and disallowed to access enterprise data and thus effectively manages app classification. App Restrictions also include use of the Windows Store, private store, auto updating, side loading, and multiple users on the same app to share data.

KNOX Workspace provides MDM APIs to install and enable applications automatically. KNOX supports Google Play, Samsung App Store, MDM, and manual side loading to deploy applications. All transactions are anonymous in an enterprise-managed model. Android requires Google Play for every app management transaction and prohibits side loading. MDM management capabilities of apps within KNOX Workspace include app installation and removal, limiting of specific app installation, disabling and enabling apps, query current app state, control app behavior, and control app notifications.

Remote Administration

MDM can query Windows 10 devices for hardware inventory, device name, username, email address, operating system and version, certificates, location, Wi-Fi MAC address, device ID, ownership designation, basic input/output system, screen resolution, OS language, and inventory of both Windows Store and non-Store apps.

MDM can query Android devices for a similar variety of information, including hardware serial number, device name, and Wi-Fi MAC address. KNOX provides additional levels of information on the workspace including installed apps.

Microsoft plans to deliver Windows 10 updates two to three times per year, although it will release new capabilities on an ongoing basis. Windows 10 gets software updates directly from Windows Update, and for Windows 10 Mobile you cannot curate updates prior to deployment. Windows 10 Mobile Enterprise allows the enterprise to curate and validate updates prior to deploying them to the user population at large.

Samsung updates KNOX without a set schedule using the over-the-air mechanism native to Android. However, these updates introduce new functionality dependent on the latest version of Android or specific hardware introduced on the latest Samsung mobile devices. For this reason, a current Samsung device may not support the latest version of KNOX, even if it does support the latest version of Android. Updates are also dependent on the carrier supporting the device, including older devices that it no longer sells.

Diagnostics and Monitoring

Windows 10 provides audit information to track issues or perform remedial actions. This information provides assurance that the device configuration complies with organizational standards. Windows 10

remote device health attestation uses measured boot data to verify the health status of the device. MDM leverages health state correlated with policies to grant conditional access based on the current state of the device. The device must prove itself to be malware-free, have security tools active and fully updated to the correct patch level, or have access denied to designated resources.

KNOX remote device health attestation measures the state of a device to make decisions about allowing the device on the trusted network. These measurements include proof that only approved system software was loaded during boot. In addition, it checks security violation logs, the KNOX Warranty Violation Bit status, and device identifying information like IMEI and Wi-Fi MAC address. It confirms that Security Enhancements for Android is running in enforcing mode and, through a locally computed verdict, identifies whether or not the device is in a trustworthy state.

Microsoft routinely gathers Windows 10 telemetry, which is system data uploaded by the Connected User Experience and Telemetry component. This is primarily anonymous data used for OS diagnostics and improving the user experience. To disable this functionality on Windows 10 Mobile, customers must upgrade to the Windows 10 Mobile Enterprise edition. Windows 10 Mobile does not allow disabling this feature. In Windows 10 Mobile Enterprise, the enterprise can configure telemetry at any of the four supported levels, including the security level. The security level gathers only the telemetry info that is required to keep Windows devices secure with the latest security updates. To prevent Windows from sending any data to Microsoft, turn off Windows Defender telemetry, Malicious Software Removal Tool reporting, and all other connections to Microsoft services. We are not aware of any additional details collected by Samsung in addition to what is already collected by Google and the mobile carrier.

Testing Scores

Management	SAL	Usability
Windows 10	**93**	**93**
KNOX 2.4	**81**	**82**

In our estimate, the management advantages brought about by KNOX 2.4.1 were little changed from the earlier version. KNOX did introduce functionality similar to Windows 10 in that both allow the use of enterprise domain accounts for automated device enrollment and configuration. The key difference, however, is KNOX is specific to the enterprise container. While this should be a significant step forward, when we actually measured it based on time to task, it shows no significant improvement in user or admin usability. The fact is maintaining a dual OS environment is simply a cumbersome process, no matter how many features it provides. Windows 10 and Samsung KNOX both support remote health attestation, which again, is the strongest value of KNOX to Android. However, where Microsoft is consistent and timely with delivering OS and security updates, Samsung is inconsistent in OS and security updates, if providing any at all for legacy devices.

Conclusion

As enterprises become more focused on mobility, they will need to have solutions that integrate the PC environment with the mobile. Built as a universal platform supporting phones, tablets, and PCs, Microsoft Windows 10 provides an all-encompassing solution, whereas Android is only a mobile OS. What's more, Samsung KNOX supports only a subset of Android phones and tablets, so it cannot provide a total solution in a multivendor Android environment. Based on Pique Solutions' lab-based comparative feature assessment of Windows 10 and Android 6 with Samsung KNOX in the security and manageability categories, we conclude that Windows 10 provides a better option for the enterprise than Android 6 with Samsung KNOX.

Samsung KNOX slightly enhances the security capabilities in Android 6 and Android for Work, but it is our belief that KNOX will benefit more from the adoption of Android 6. Unlike KNOX, or Android, Windows 10 integrates security and management capabilities in the operating system itself rather than packaging them as an add-on. Both Windows 10 and Samsung KNOX provide health attestation reports of the device's integrity to an MDM system to ensure the device meets enterprise compliance requirements.

KNOX still depends on Android for many things, and Windows 10 scores higher than Android in every category. KNOX 2.4 does offer support for enterprise AD and fingerprint biometrics for authentication in the KNOX secure container. KNOX 2.6 is slated to support the Android API for fingerprints. With Windows 10, however, authentication is not limited to the OS but includes support for everything. More importantly, Windows 10 has already adopted FIDO 2.0 for authentication for the enterprise and for consumers. Windows is still the more resilient platform providing the highest levels of security assurance and the lowest impact on usability when implementing this level of assurance, a very strong distinction.

