PIQUE SOLUTIONS

Choosing the Best Tablet for the Enterprise

A Comparison of Windows 8.1 Pro and Samsung KNOX™-Enabled Tablets

April 2014

THE DEVELOPMENT OF THIS WHITE PAPER WAS SPONSORED BY MICROSOFT, BUT THE UNDERLYING RESEARCH AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | Fax: 415.373.3892

Contents

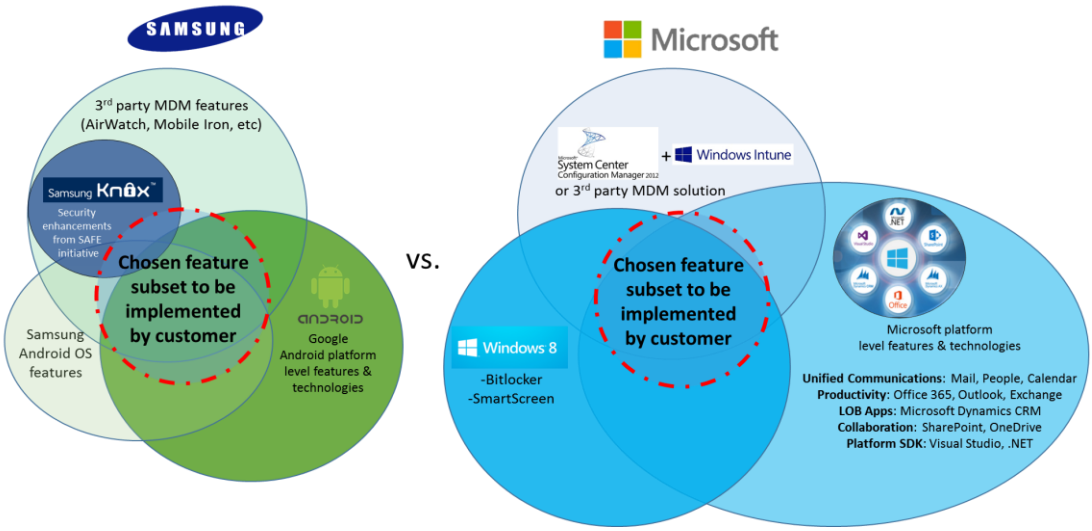
Executive Summary

If there is one lesson that we have learned from the mobile revolution that started in the consumer space and is now manifesting itself in the workplace, it is that users demand choice with regard to their technologies and platforms. The adoption of tablet computers for around-the-office use is one of the most important developments we have seen in recent years. However, in taking products designed for consumer environments, and using them for enterprise tasks, we often discover that enterprise requirements for security, reliability, and functionality are far more demanding than what we find in the consumer space. This is particularly true when we see the rapid adoption of tablets in security-sensitive environments such as finance and healthcare where security breaches can have most severe repercussions.

Pique Solutions and its strategic partner Miratech, a global systems integrator with a dedicated enterprise mobility services practice, conducted an exhaustive lab-based evaluation of Windows 8.1 Pro and Samsung KNOX™ on tablet PCs. This study matched the capabilities of a Windows Surface Pro 2 tablet running Windows 8.1 Pro against a Samsung Galaxy Note 10.1 (2014 Edition) running Android™ 4.3 ("Jelly Bean") and Samsung KNOX, and looked at a number of areas important to enterprise users. While a Surface Pro 2 tablet was used for this test, the capabilities described would be available in any tablet running Windows 8.1.

As pictured in **Figure 1** below, the comparison revealed that Samsung KNOX can only be delivered as part of an enterprise solution involving multiple vendors while the Microsoft enterprise mobility platform provides an environment that is cohesive, comprehensive, and integrated.

Figure 1. Samsung vs. Microsoft Enterprise Solutions



The testing showed that KNOX offers some advantages, particularly with regard to dual-persona support or the ability to partition the device into work and personal spaces. Overall, however, it lags behind Windows 8.1 Pro in security, platform-level features, and the integration with the full Microsoft tool set including Office, SharePoint, Exchange, and Lync. Moreover, Samsung KNOX includes features that overlap with features already offered by established Mobile Device Management (MDM) market leaders such as MobileIron and AirWatch, leaving enterprise customers uncertain as for which feature set and MDM vendor they should use.

Based on this review, it is our opinion that KNOX was a necessary addition to the Android environment and provides a degree of protection in enterprise Android deployments. KNOX has addressed some of the more glaring security problems that have plagued Android, but the jury is still out on whether the platform is now truly "enterprise-grade." What is clear is that the requirements for an enterprise-grade tablet go beyond the need to meet the basic capabilities for enterprise security. A Windows 8.1 Pro tablet can deliver a fun and engaging user interface for simple tasks such as e-mail, web surfing, and media consumption, but still serve as a fully functioning Windows computer for more intensive enterprise work. Solutions based on Microsoft Windows remain the best choice for enterprise users, as they deliver on the most stringent security, productivity and compatibility requirements.

While users have embraced their mobile devices, security exposure remains a major concern for CIOs, particularly on the Android platform. In an attempt to address these concerns, software developers and device manufacturers have tried to develop solutions to shore up the inherent deficiencies in the Android platform. Yet the degree to which they succeeded is still a matter of debate, as some of the underlying security weaknesses of the Android platform might still put users at risk despite the KNOX add-on.[1]

Introduction

While Windows 8.1 Pro is designed around the robust security capabilities users have come to expect from desktop computers, Android was built on the premise of an open operating system that Google has encouraged manufacturers and developers to adopt and enhance. This collaborative environment and diversity of manufacturer base has launched Android to the front in terms of consumer mobile operating systems, but it has also made Android the prime target for mobile malware. That exposure increases exponentially if the device has been "rooted", the process whereby the inherent security mechanisms are disabled, allowing any software to gain administrative privileges. As McAfee's Consumer Mobile Trends Report from June 2013 states, "6 of the top 10 worst malware in China involved rooting software".

The ability for a user to root their Android device with relatively simple tools available on the web creates a significant exposure. Couple that with the growing library of Android malware and you have the "perfect storm" threating enterprise security. As the McAfee Labs Threats Report: Third Quarter 2013 reads in part, "To speak of malware that infects mobile devices is to speak of Android malware. Threats against other mobile operating systems … are insignificant compared with malicious Android apps. This quarter our count of Android malware grew by one-third, to more than 680,000 samples."

[1] For a recent report on an alleged successful Man in the Middle (MitM) attack on the Android platform with Samsung KNOX, see the article *Information stored in glass houses won't be protected by Samsung locks* published by Betanews, March 21, 2014.

Recognizing the challenge of getting enterprises to adopt Android, some device manufacturers and independent software vendors found an opportunity to provide software tools for the Android environment to address the security and management concerns of enterprise IT departments; Samsung has clearly been in the forefront of those activities even while the entire endeavor may be built on shaky ground.

Early versions of Android (i.e. pre-Android 3.0 or "Honeycomb") lacked such basic security mechanisms as on-device encryption. While those glaring deficiencies have been addressed in subsequent releases, there are still seven different Android releases in circulation and no published schedule for updates. Therefore, Android still presents some significant security challenges for enterprises, particularly with the potential for rooting and the introduction of software of unknown origin.

Recognizing an opportunity in the enterprise mobility market with the demise of BlackBerry, Samsung set about to develop tools that would result in an "enterprise-grade Android", and help differentiate its implementation from other manufacturers' versions of Android. Its first foray was the Samsung for Enterprise (SAFE) program that provided support for Microsoft Exchange ActiveSync IT policy control through third-party Mobile Device Management (MDM) solutions, and virtual private network (VPN) connectivity along with on-device encryption.

In February 2013, Samsung moved to increase Android's security profile with the announcement of its enterprise mobile security platform, KNOX. KNOX added a number of security capabilities to SAFE, including platform security and data/application security. The platform security measures include a Customizable Secure Boot function that ensures only verified and authorized software can run on the device. The secure boot function operates in conjunction with the TrustZone Integrity Management Architecture (TIMA) that detects when the integrity of the kernel or the boot loader is violated. There is also a remote attestation feature that allows IT administrators to verify the authenticity and integrity of KNOX devices during and after enrollment. Those capabilities are not required in the Windows 8.1 Pro architecture where each application is isolated in its own container.

The other key capability of KNOX is its secure container technology designed to protect data and applications. Long a staple among third-party MDM manufacturers, a secure container (or "sandbox") is a software-defined region within the device where corporate data and applications can be isolated from the user's personal information. Steps can be taken so that data delivered to the secure container cannot be forwarded or copy-and-pasted to other non-secure regions. Furthermore, if the device is lost or stolen or if the user leaves the organization, an IT administrator can remotely wipe the entire device or just the corporate data.

However, as previously referenced, researchers at Cyber Security Labs of Ben-Gurion University of the Negev (BGU) claim that they have been able to access information secured in a Samsung KNOX environment by redirecting the network connection in the underlying Android software. The penetration did not attack the secure container itself, but rather intercepted traffic as it flowed out of the secure container and before it was encrypted by the network stack. The result, the researchers assert, was a classic Man in the Middle (MitM) attack to access unencrypted data while it was flowing out of the secure container.

Samsung announced the availability of KNOX in late 2013, initially making KNOX available on just four mobile devices: the Galaxy S4, Galaxy Note 10.1 (2014 edition), the Galaxy Note 3 "phablet," and the Galaxy S III smartphone. However, KNOX can run only on certain carriers' models of the Note 3 and S4. According to eWeek (February 2014), of the 25 million Samsung Android devices that have shipped

since KNOX became available, only 1 million are running KNOX.

At the Mobile World Congress in February 2014, Samsung announced an enhancement to the KNOX program called KNOX 2.0. The enhancement provides real-time kernel protection against malicious attacks, and allows the container to run unmodified Android applications, eliminating the need for application wrapping. It also allows controlled data sharing between the personal space and the secure container. The TrustZone capabilities are expanded to handle cryptography keys and client certificates, and a multi-vendor VPN framework was added to support third-party clients including SSL VPN. Finally, KNOX 2.0 adds an open SmartCard framework allowing enterprises to choose from an array of smartcard readers.

The upgraded version is planned for delivery in the second quarter of 2014. The company has promised the number of KNOX-capable devices will triple during 2014; it has yet to publish a detailed list or timetable.

Testing Methodology

The overall plan for the testing methodology developed by Pique and Miratech was to:

1. List all the mobility capabilities that would be important for enterprise use in a consistent testing framework.
2. Design and build a testing lab to imitate a real-world enterprise environment.
3. Use devices that are widely available on the retail market and would be the most likely candidates to be used in the enterprise environment.
4. Manually confirm how the selected devices perform in the tasks defined in the testing framework.
5. Develop a detailed report of the results.

The resulting testing framework included 345 criteria, distributed across the following six functional areas:

- **Unified Communications Functionality**: E-mail, Calendar, Contacts, Microsoft Office, integration to Microsoft Exchange and Microsoft SharePoint.
- **Exchange ActiveSync Support**
- **Network Services Functionality**: Network and communication protocols and technologies support.
- **Mobile Device Management (MDM)**: Capabilities related to enterprise device management via MDM systems – remote access, blacklisting of the apps, remote wipe etc.
- **System and Data Security**: Protection from unauthorized access, virus and malware protection, data encryption, etc.
- **Platform Functionality**: Development tools, frameworks, licensing, support, etc.

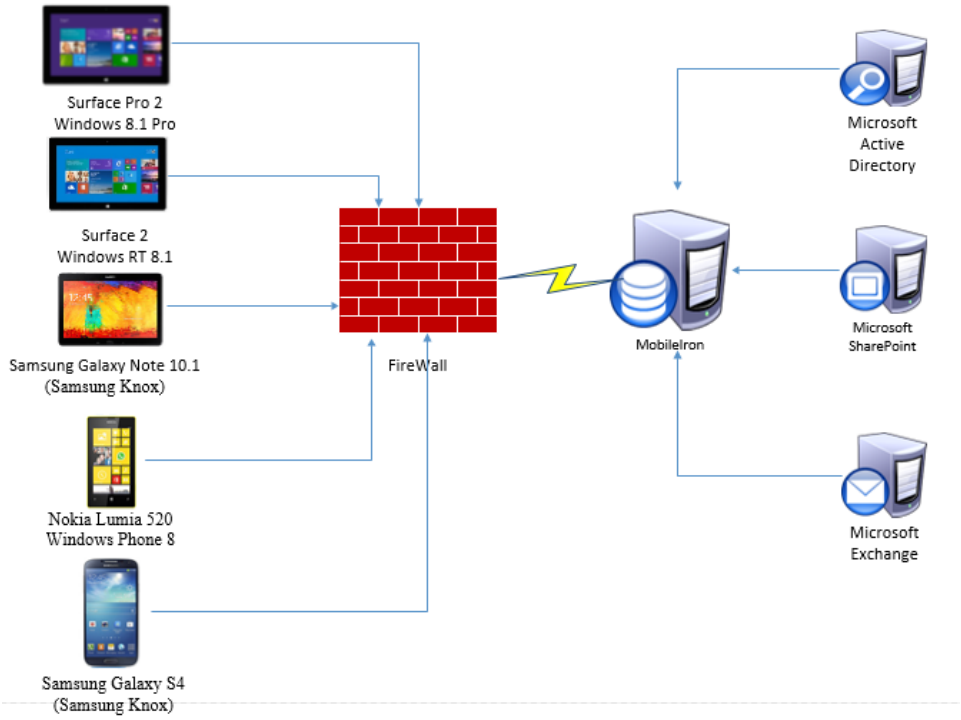
Each feature was scored on a scale of 0 to 5 where “0” indicated a complete absence of the feature and “5” indicated the highest level of its functionality.

Pique and Miratech also took the approach of recognizing that not all the features are equally important in the enterprise mobility. For example, the ability to disable e-mail address autocomplete is much less important than the availability of built-in antivirus. To address these differences, each criterion was ranked based on its importance for enterprise mobility, using a scale of 1 to 5 where “1” indicated “Not important” and “5” indicated the highest level of importance. To combine the two

elements, the “Functionality” scores were multiplied by the “Importance” rankings to arrive at a weighted score for each of the criteria.

To imitate the real enterprise environment, Miratech built a mobile testing lab using the design portrayed in **Figure 2**:

Figure 2. Mobile Lab Testing Environment



1) For the testing environment, we used the most widely adopted software in the enterprise world: Microsoft Windows Server, Microsoft Active Directory, Microsoft Exchange, and Microsoft SharePoint.
2) The MDM system used was MobileIron, integrated with the set of Microsoft tools.
3) The devices used were:
    a. Microsoft Surface Pro 2 (Windows 8.1 Pro)
    b. Microsoft Surface 2 (Windows 8.1 RT)
    c. Samsung Galaxy Note 10.1 (Android 4.3 with KNOX)
    d. Samsung Galaxy S4 (Android 4.3 with KNOX)

The enterprise mobility specialists configured the test environment as well as the devices, executed all the scenarios defined in the testing framework, and developed the resulting report with a quantitative comparison of the platforms.

Testing Results

Based on the extensive testing we conclude that, while Samsung KNOX security enhancements succeeded in addressing some of the Android security deficiencies, its security capabilities are inferior to those that the native Windows 8.1 Pro delivers out-of-the-box. Furthermore, while Windows’ security capabilities have been developed and tested on hundreds of millions of devices over decades, Android and particularly KNOX are still relative newcomers who have not been challenged to the same

degree yet. The alleged successful Man in the Middle (MitM) attack launched by the Cyber Security Labs of Ben-Gurion University of the Negev and referenced earlier, is a perfect illustration of that.

Among the key advantages of the Windows 8.1 Pro implementation were:

- Native support for key security requirements without the need for additional software.
- Integrated, out-of-the box antivirus and firewall capabilities.
- Unified Extensible Firmware Interface (UEFI) secure boot function making it essentially impossible to introduce unapproved software.
- An architecture where each application runs in an isolated area with managed inter-app communication eliminating the need for a specific secure container.
- Built-in BitLocker data encryption capability.
- SmartScreen technology to validate websites visited.
- Flexible certificate management.
- Seamless integration with an existing Active Directory / Exchange / SharePoint / System Center Configuration Manager environments.
- Immediate support for any existing software developed for Windows desktops and laptops.
- A tablet that is 100% compatible with all the existing infrastructure and management tools.
- Single vendor enterprise-class 24/7 support (the same as with other enterprise systems).

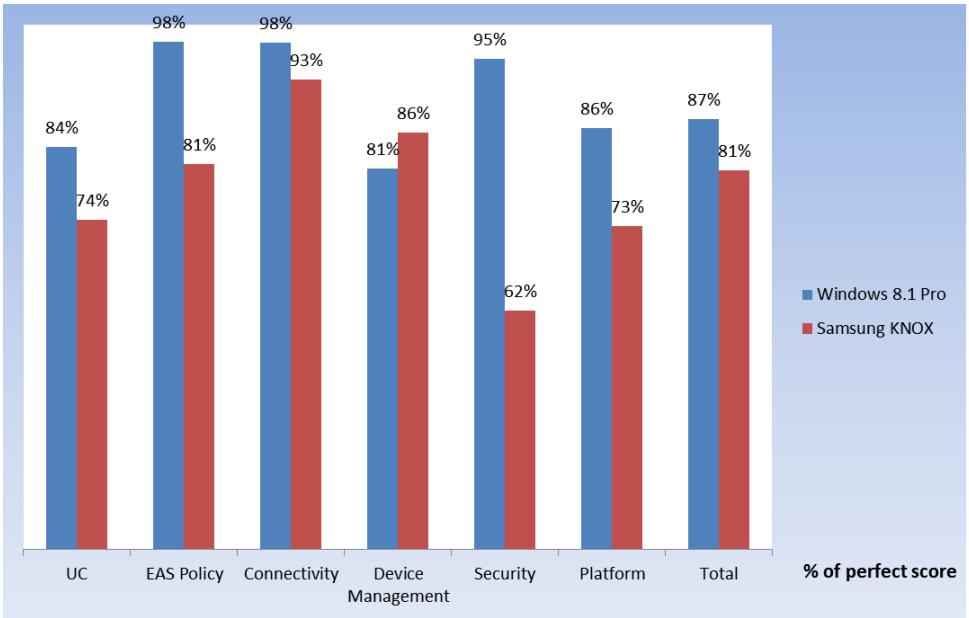
As shown in **Table 1**, the analysis compared the two platforms with regard to 345 separate criteria addressing security, platform and services functionality, device-management capabilities, unified-communications functionality and for enterprise users the all-important integration with the Microsoft toolset including Office, SharePoint, and Exchange Active Sync.

Table 1. Testing Criteria by Functional Areas

Functional Area	Number of Criteria Examined
Unified Communications Functionality	42
Exchange ActiveSync Support	43
Network Services Functionality	42
Mobile Device Management (MDM)	155
System and Data Security	33
Platform Functionality	30

Figure 3 shows a summary and comparison of how the Windows 8.1 Pro and Samsung tablet with KNOX compared in the six categories tested. The percentages represent how the scores achieved by Windows 8.1 Pro and Samsung KNOX compared to a "perfect score" in each category (i.e. the highest possible "Functionality" score of 5 multiplied by the highest "Importance" ranking of 5).

Figure 3. Summary of Lab Testing Results (percentages of perfect scores)



The testing identified the most dramatic difference between Windows 8.1 Pro and Samsung KNOX in the System and Data Security category where Windows achieved 95% of perfect score versus 62% for KNOX. Windows scored higher in all categories except for Mobile Device Management (MDM), where KNOX led Windows by 5% due to a richer set of MDM features.

Table 2 shows a comparison of the sum of the simple scores (i.e. the raw "Functionality" scores) for Windows 8.1 Pro versus the Samsung tablet with KNOX.

Table 2. Evaluation of Windows 8.1 Pro vs. Samsung KNOX (simple scores)

Category	Windows 8.1 Pro	Samsung KNOX
Unified Communications	180	159
Exchange ActiveSync Support	210	175
Network Services	200	190
Mobile Device Management (MDM)	618	655
System and Security	210	136
Platform Functionality	125	106
Total Score	**1,543**	**1,421**

Table 3 shows a comparison of the sum of the weighted scores (i.e. "Functionality" scores multiplied by the "Importance" ranking) for Windows 8.1 Pro versus the Samsung tablet with KNOX. The advantages of Windows over KNOX became more apparent with this approach, indicating that Windows is particularly strong in the capabilities most important to enterprises.

Table 3. Evaluation of Windows 8.1 Pro vs. Samsung KNOX (weighted scores)

Category	Windows 8.1 Pro	Samsung KNOX
Unified Communications	725	616
Exchange ActiveSync Support	895	760
Network Services	910	860
Mobile Device Management (MDM)	2,602	2,729
System and Security	1,005	592
Platform Functionality	528	445
Total Score	**6,665**	**6,002**

Next, we shall look specifically at the key differences uncovered in each of these areas.

Unified Communications Functionality

Unified Communications Functionality			
Windows 8.1 Pro		**Samsung KNOX-Enabled Tablet**	
Simple Score	Weighted Score	Simple Score	Weighted Score
180	725	159	616

The major advantage of Windows 8.1 Pro revolves around the synergy it has with the full Windows enterprise tool set. Virtually all tablet users engage in web browsing, e-mail, and media consumption, but enterprise users need access to the full range of productivity tools to make full use of a tablet in their business lives. It is in that area where we find some of the biggest advantages for Windows over Android, with or without KNOX.

Windows 8.1 Pro is designed to work seamlessly with the main "must have" business app in the enterprise world, Microsoft Office. Though Microsoft Office is licensed separately, together with Windows 8.1 Pro the two make a combination that can greatly boost knowledge worker productivity. Rather than the full Office suite, Samsung's Android implementation relies on the less functional Polaris® Office.

With Windows 8.1 Pro, the full suite of standard Mail, People, Calendar, Photo, and other built-in apps are simpler, faster and more functional. Calendar is especially powerful with its integration to e-mail, contacts and other business productivity tools. One good example is the calendar's ability to allow a

user to organize a meeting with any of the global contacts and choose available meeting rooms just as they would from a desktop.

As many users do personal as well as business tasks on their tablets, Windows 8.1 Pro allows them to combine Outlook, Gmail, and Yahoo! accounts and allows the user to manage all of them from a single point.

Exchange ActiveSync Support

Exchange ActiveSync Support			
Windows 8.1 Pro		**Samsung KNOX-Enabled Tablet**	
Simple Score	Weighted Score	Simple Score	Weighted Score
210	895	175	760

Probably the most widely used enterprise productivity tool today is Exchange ActiveSync that synchronizes e-mail, contacts, calendar and tasks among all of the user's fixed and mobile devices. Windows 8.1 Pro provides access to an extensive set of management features for shared file resources available to Microsoft Exchange ActiveSync users.

For additional control, Windows 8.1 Pro supports the ability to allow or deny access to Non-Provisionable Devices that do not support the full set of policies on Exchange 2010 via Exchange ActiveSync. That capability provides controlled support for older devices. It also supports a Maximum Calendar Age Filter, which defines the number of calendar days to be synced to the device.

For application management, Windows 8.1 Pro can allow or disallow Unsigned Applications, Unsigned Installation Packages, and Unapproved InROM Application Lists. Windows 8.1 Pro also supports Approved Application List, which prevents the device from running apps that are not on the whitelist. These policies work only with an Exchange Enterprise client license.

Network Services Functionality

Network Services Functionality			
Windows 8.1 Pro		**Samsung KNOX-Enabled Tablet**	
Simple Score	Weighted Score	Simple Score	Weighted Score
200	910	190	860

While both platforms support a range of virtual private network (VPN) options for securely transferring information over a network, Windows 8.1 Pro supports two very important additions to that list, EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) and EAP-GTC (Generic Token Card). The PEAP-EAP-TLS (Protected Extensible Authentication Protocol-EAP-TLS) protocol is used for certificate-based authentication in many environments. PEAP-EAP-TLS allows organizations to use smart-card authentication and provides a mutual identity check, negotiation of encryption method, and key determination between the client and the authentication authority.

EAP-GTC protocol supports authentication with cards bearing digital certificates on an embedded electronic board. Further, GTC has the option of hiding the user's identity details when using TLS to prevent the user's name from being broadcast during the authentication phase.

Mobile Device Management

Mobile Device Management			
Windows 8.1 Pro		**Samsung KNOX-Enabled Tablet**	
Simple Score	Weighted Score	Simple Score	Weighted Score
618	2,602	655	2,729

In enterprise environments, mobile devices are often administered and managed by a Mobile Device Management (MDM) system; the use of KNOX actually requires a third-party MDM system. Windows 8.1 Pro allows for complete management of the device with built-in support for the Open Mobile Alliance Device Management (OMA-DM) that exposes the necessary device controls for third-party MDM solutions.

In configuring the MDM policies, Windows 8.1 Pro tablets may be connected to Active Directory (AD) with full support of all of its major policies. In addition, synchronization with AD provides a single management point for existing and future enterprise employees' profiles and data, eliminating the need to set up profiles in multiple places.

If the organization uses Microsoft management tools, the System Center Configuration Manager (SCCM) enables centralized deployment of apps and software updates on all devices; with the addition of Intune, SCCM can support iOS and Android devices as well. The use of Active Directory domain features simplifies the device management in enterprise deployments, and provides detailed information regarding certificates along with management tools for modifying, deleting and installing certificates.

System and Data Security

System and Data Security			
Windows 8.1 Pro		**Samsung KNOX-Enabled Tablet**	
Simple Score	Weighted Score	Simple Score	Weighted Score
210	1,105	136	592

Many of the security capabilities for Windows 8.1 Pro stem from that fact that Windows was developed initially as a desktop/laptop operating system and then enhanced with touch screen capabilities to deliver a full user experience on tablets. To begin with, Windows 8.1 Pro comes standard with built-in antivirus-malware protection through Windows Defender. Windows 8.1 Pro features a Unified Extensible Firmware Interface (UEFI) safe boot function to block malware and viruses upon boot. With

the safe boot function, the antivirus software is loaded before third-party drivers or applications. The hardware is protected with the Trusted Platform Module (TPM), and secured using TPM key attestation.

With KNOX, Samsung has added a similar capability to Android: KNOX's Customizable Secure Boot function ensures that only verified and authorized software can run on the device. The secure boot function operates in conjunction with the TrustZone Integrity Management Architecture (TIMA), a function of ARM that can detect when the integrity of the kernel or the boot loader is violated, and take steps to halt the booting process. Even with Secure Boot, any end user can change the boot image. This alters the hardware, voids the device warranty, and causes KNOX to stop working. The device still functions with the user image, but corporate data becomes inaccessible and a new KNOX container can no longer be created on such a device.

For data protection, Windows 8.1 Pro incorporates BitLocker and BitLocker To Go file system encryption. BitLocker provides software encryption for the entire volume, individual files and folders, as well as removable storage devices. BitLocker also supports Enhanced Storage with HDD encrypting of every physical block on the disk. By default, it uses the AES encryption algorithm in CBC mode with a 128-bit or 256-bit key. The encryption function is implemented in hardware in the disk controller.

In its secure container technology, KNOX configures a software-defined region within the device where corporate data and applications are isolated from the user's personal information. Steps are taken so that data delivered to the secure container cannot be forwarded or copy & pasted to other non-secure regions. Like BitLocker, KNOX employs 256-bit AES encryption. With either platform, if the device is lost or stolen or if the user leaves the organization, an administrator can remotely wipe the entire device or just the corporate data. Windows 8.1 Pro provides this through Remote Business Data Removal, while KNOX relies on the remote wipe capability provided in the third-party Mobile Device Management (MDM) system that must be implemented with it.

Along with blocking malware and encrypting corporate data on the device, Windows 8.1 Pro includes Microsoft's SmartScreen technology to help protect users against attacks that utilize social engineering and from drive-by downloads that can infect a system when browsing. SmartScreen does this by scanning URLs accessed by a user and checking them against a blacklist of websites containing known threats. SmartScreen also provides application reputation monitoring and scans websites to detect the use of binary extensions.

Finally, for device access, Windows 8.1 Pro on the Surface Pro 2 tablet provides true purpose-built touch-based fingerprint biometrics rather than Samsung's cobbled together fingerprint scanning capability using the built-in camera and separate analysis software.

Platform Functionality

Platform Functionality			
Windows 8.1 Pro		**Samsung KNOX-Enabled Tablet**	
Simple Score	Weighted Score	Simple Score	Weighted Score
125	528	106	445

From a developer's standpoint, the Windows 8.1 Pro powerful SDK provides the tools to develop and execute virtually any task required by a user.

No additional SDKs or third-party tools are required. Windows 8.1 Pro provides developers with the unique choice of frameworks, languages and development tools for any purpose including:

- C++, JavaScript, .NET Framework, C#, Visual Basic
- User Interface (UI) technologies: XAML, HTML, DirectX, and
- Windows Store business models
- Visual Studio Express 2013 for Windows 8.1 Pro, a free lightweight version of Visual Studio that comes with Blend. Blend allows developers to build the UI with XAML or HTML5 / CSS3, and provides visual design tools, data binding, styling and theming, etc.

For applications maintenance, Windows 8.1 Pro can update all the apps from the Windows Marketplace automatically and in the background; this capability will work even when the device is in sleep mode. Windows 8.1 Pro multitasking is improved with the WinJS scheduler that allows high-priority tasks to be handled in a priority fashion.

Finally, Windows 8.1 Pro strives to deliver the best browsing experience with Internet Explorer 11. Internet Explorer 11 ensures security and confidentiality when surfing with several new features:

- Improved password management
- Enhanced Protected Mode: Offering protection from socially-engineered attacks, attacks designed to exploit vulnerabilities in Web sites, and attacks designed to exploit the browser or operating system
- Encryption API
- Improved SmartScreen filtering

Business Case Analysis

Along with the analysis of the Windows 8.1 Pro and Samsung KNOX capabilities, Pique Solutions reviewed the published literature and interviewed representatives of two of the major Mobile Device Management (MDM) vendors regarding the strengths and weaknesses of the two platforms. In the end, we found a number of questions enterprise buyers should be considering regarding the choice of a Samsung tablet with KNOX as a functional and secure enterprise platform. Key among those would be:

- Why would Samsung develop a capability that partially overlaps with what is already available from the Mobile Device Management (MDM) vendors?
- Is KNOX really a necessity for enterprises deploying Android mobile devices?
- Is Android with the addition of KNOX a good option for enterprise mobility?

With regard to the “why” of KNOX, it is clear that Samsung has listened to the concerns of skeptical enterprise IT buyers who were well aware of the security deficiencies in the Android platform. The BYOD revolution came as a shock to enterprise IT that was now forced out of the comfort zone provided by the ironclad security envelope of a BlackBerry environment. The iPhone represented the first wave of those user owned devices, and while the first two versions of iOS lacked key enterprise security mechanisms like on device encryption, by the release of iOS 3 in 2009 Apple was providing the types of capabilities enterprises were demanding.

Google was slower to respond to those enterprise requirements. The first version of Android that supported on device encryption was 3.0 “Honey Comb” released in February 2011. However, Honey Comb was exclusively a tablet operating system, and smartphone users had to wait for Android 4.0 “Ice Cream Sandwich” in October of that year to have access to on device encryption. For those earlier versions of Android, third-party encryption tools, the most popular being from 3LM, could provide that capability, however 3LM’s product was not supported on the Samsung platform.

As Samsung grew to be the world's largest supplier of Android consumer smartphones, the pressure for IT departments to support them increased creating heightened tension with enterprise security professionals. In short, Samsung needed a better security solution, and saw an opportunity to differentiate itself from other Android manufactures. Further, it saw an opening to step in with an enterprise-grade version of Android to fill the void created by the wholesale defection from BlackBerry. Samsung even created a new division, staffed largely with BlackBerry veterans, specifically tasked with increasing enterprise sales.

As to whether KNOX is "necessary" depends on the nature of the threats one is looking to thwart. KNOX delivers two primary protections: a customizable secure boot and an on-device secure container. Most of the market's attention was drawn to the secure container that created an isolated, encrypted partition on the device that could be maintained and, if need be, remotely wiped by a third-party MDM system. Many of the leading MDM platforms including AirWatch (now being acquired by VMWare), MobileIron, and Fiberlink (now being acquired by IBM) can manage KNOX devices. The focus appears to have been drawn to that capability because most of the MDM vendors already offered a secure container solution so the concept was familiar.

The downside with the KNOX secure container technology is that Samsung charges an additional $3.60 per device per month for that capability, in addition to the cost of the MDM solution. AirWatch is one of MDM providers that publishes pricing information. Its Secure Content Locker and App Wrapping capabilities are included in its top end Blue Management Suite, which lists for $6.25 per device per month. The difference between that package and the Orange Management Suite that does not include those functions is $1.25 per device per month. Therefore, you can get AirWatch's secure container solution for less than half the price of Samsung's. In any event, Windows 8.1 Pro devices can be supported on whichever desktop/laptop management solution an organization has in place, without the incremental cost of an MDM system.

However, the Customizable Secure Boot function in KNOX does provide protection against loading malicious code onto the device, and malware is a serious threat on the Android platform. The TrustZone Integrity Management Architecture (TIMA) can detect if the integrity of the kernel or the boot loader has been violated, and it can halt the booting process. As Google does not vet applications it distributes through the Google Play store, the result is that malware has run rampant in the Android environment. With KNOX, enterprises will have a better protection against malware. Again, that capability is not required in the Windows 8.1 Pro architecture where each application is isolated in its own container.

While KNOX does provide an additional level of security on Android devices, it is important to remember that there is more to enabling enterprise mobility than simply avoiding catastrophe. Users are drawn to the fun and convenience of tablets for their ability to do the types of routine tasks we find in the consumer world. Those would include e-mail, web surfing, perusing social media sites, and media consumption. Enterprise users will employ tablets for those same tasks; however, they also need the highest functionality of the productivity applications on which they depend in their business lives.

Given the success Android tablets have had in the consumer world, enterprise IT departments may face a challenge in getting users to look at the differences that exist between the platforms in working with the essential business productivity tools. One can list the feature differences; however, unless a user can experience what it is like to use the tools in their everyday work lives, it could be a tough sell.

The enterprise represents an entirely different environment with a different set of imperatives. With the exception of the System and Data Security capabilities where Windows significantly outperformed KNOX, the inclusion of KNOX can put a Samsung Android device on a seemingly equal footing with a Windows 8.1 Pro tablet. However, we do see a distinct difference in how the two perform in a business

environment. Easier integration with productivity and collaboration tools such Office, SharePoint, Exchange, Lync, as well as line-of-business (LOB) applications such as Microsoft Dynamics puts Windows at a distinct advantage when it comes to worker productivity. Also important are Windows' SDK capabilities and support for functions like Active Directory and System Center CM.

In the end, when comparing the costs and capabilities of the native Windows 8.1 Pro versus the add-on KNOX capabilities and the overall user experience in working with the key business productivity applications, a very compelling argument can be made for selecting Windows. Convincing users that Windows 8.1 Pro can match the Android experience for consumer tasks may take a hands-on demo. However, it is a far more challenging prospect to take a consumer-oriented platform and adapt it for actual enterprise use. When you start with the premise that enterprise tablets are for enterprise work, Windows wins decisively.

Conclusions and Guidance

While they got their start in the consumer market, the use of tablets as an alternative enterprise platform is growing at least for less keyboard-intensive tasks. That transition from consumer to enterprise has exposed many of the deficiencies of tablets in terms of both security and functionality. Delivering that fun and engaging tablet interface to enterprise users while also providing the productivity enhancing functions that justify enterprise use requires getting both of those aspects in hand.

The mobile revolution has clearly demonstrated that users want choice. Whether it is in terms of screen size, operating system, hardware platform, or range of functionality, one will scarcely find a tablet device that meets the needs and preferences of every user. Further, while user satisfaction is one goal to be sought, in the enterprise that must be counterbalanced with the need to secure corporate data and systems.

It is important to recognize that not all users will grasp the fact that consumer tablets will not necessarily allow them to do all the things they need to do when it comes to enterprise work. In the end, the primary goal in enterprise computing is still enhanced productivity. Regardless of whether the tablet is company-provided or user-owned ("BYOD"), CIOs and IT Managers should take the opportunity to counsel users on their device selection to ensure that they consider the entire range of work-related tasks they will aim to accomplish.

Given the overwhelming consumer focus in the mobility market, the need for those essential business functions is often drowned out. Most tablets deliver a compelling user experience when tasked with supporting the regular line up of consumer tasks, but they can falter when tackling the day-to-day work requirements. As tablet selection is easily swayed by considerations regarding consumer applications, it is important to expand the discussion and educate users about the importance of enterprise productivity tools so that in the end they are truly satisfied with the tablet they select.

Based on the results of extensive testing, and taking into account the full complement of out-of-the-box enterprise security and management capability and the ability to interact seamlessly with the entire Microsoft productivity suite, we conclude that the Windows 8.1 Pro tablet offers a superior alternative to the Samsung tablet with KNOX for bridging the consumer and enterprise requirements. With the touch screen interface and active tiles interface, Windows 8.1 Pro delivers an engaging tablet experience, but with support for a full Windows operating system (with extensive touch capabilities) it can serve as a viable alternative to a laptop or desktop for more intensive functions, or simply serve as a convenient option in a mobile scenario. Finally, as with Android tablets, Windows 8.1 Pro can be run on a wide variety of hardware platforms offering different configurations, form factors, peripherals, and price points.

To be sure, tablets are here to stay, and while all consumer tablets may be created roughly equal, the same cannot be said for enterprise tablets.

Appendix: Device Specifications

Table 1. Microsoft Surface Pro 2 Device Specifications

OS	Runs Windows 8.1 Pro with one month trial for new Microsoft Office 365 customers. Download apps from the Windows Store. Also runs Windows 7 desktop applications and integrates with your existing enterprise management infrastructure.
Exterior	10.81 x 6.81 x 0.53in; 2lbs; VaporMg casing; Dark Titanium color; Volume and Power buttons
Storage	64GB*, 128GB**System software uses significant storage space. Available storage is subject to change based on system software updates and apps usage.
Display	10.6" Clear Type Full HD Display; 1920 x 1080 pixels; 16:9 (widescreen); 10-point multi-touch
Pen Input	Pen input and pen (included with purchase)
CPU	4th Gen 1Intel® CoreTMi5 Processor with Intel HD Graphics 44004GB RAM—Dual Channel Memory
Wireless	Wi-Fi (802.11a/b/g/n)
	Bluetooth 4.0 Low Energy technology
Battery	
Cameras and A/V	Two 720p HD LifeCams, front-and rear-facing with True Color
	Microphone
	Stereo speakers with Dolby(R) sound
Ports	Full-size USB 3.0; microSDXC card reader; Headset jack; Mini DisplayPort; Cover port
Sensors	Ambient light sensor; Accelerometer; Gyroscope; Compass
Power Supply	48W power supply (including 5W USB for accessory charging)
Warranty	1-year limited hardware warranty
Apps (included)	Mail, Calendar, People, Internet Explorer 11,Photos, Camera, Music, Video, Games, Skype, SkyDrive, News, Weather, Sports, Travel, Finance, Health & Fitness, and more.

Table 2. Samsung Galaxy Note 10.1 2014 Edition Device Specifications

Body	Dimensions	243.1 x 171.4 x 7.9 mm (9.57 x 6.75 x 0.31 in)
	Weight	540g (WIFI)/ 535 g (3G)/ 547g (LTE) (1.18 lb)
		- S Pen stylus
Display	Type	Super clear LCD capacitive touchscreen, 16M colors
	Size	2560 x 1600 pixels, 10.1 inches (~299 ppi pixel density)
	Multitouch	Yes, up to 10 fingers
		- Samsung TouchWiz UI
Sound	Alert types	Vibration; MP3, WAV ringtones
	Loudspeaker	Yes, with stereo speakers
	3.5mm jack	Yes
		- Dolby mobile sound enhancement
Memory	Card slot	microSD, up to 64 GB
	Internal	16/32/64 GB storage, 3 GB RAM
Data	GPRS	Yes
	EDGE	Yes
	Speed	HSDPA, 42 Mbps (LTE model), 21 Mbps (3G model); HSUPA, 5.76 Mbps; LTE, Cat4, 50 Mbps UL, 150 Mbps DL
	WLAN	Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, Wi-Fi hotspot
	Bluetooth	Yes, v4.0 with A2DP
	Infrared port	Yes
	USB	Yes, microUSB v2.0, USB Host
Camera	Primary	8 MP, 3264x2448 pixels, autofocus, LED flash, check quality
	Features	Geo-tagging, face and smile detection
	Video	Yes, 1080p@60fps (LTE model), check quality
	Secondary	Yes, 2 MP, 1080p@30fps

Features	OS	Android OS, v4.3 (Jelly Bean)
	Chipset	Qualcomm Snapdragon 800
	CPU	Quad-core 2.3 GHz Krait 400 (LTE model)/ Quad-core 1.9 GHz Cortex-A15 & quad-core 1.3 GHz Cortex-A7 (3G model)
	GPU	Adreno 330 (LTE model)
	Sensors	Accelerometer, proximity, compass
	Messaging	SMS(threaded view), MMS, Email, Push Mail, IM, RSS
	Browser	HTML5
	Radio	No
	GPS	Yes, with A-GPS support and GLONASS
	Java	Yes, via Java MIDP emulator
	Colors	Black, White
Battery		Non-removable Li-Po 8220 mAh battery
	Stand-by	Up to 2230 h
	Talk time	Up to 10 h (multimedia) (2G) / Up to 49 h (3G)
	Music play	Up to 98 h