



Smartphones, Security and the Enterprise:
The Equation to Solve

IT departments need to think long and hard before deciding on the right smartphone platform for their business needs.

CONTENTS

The User Revolution	2
Risk/Reward: A Complex Equation	3
Making Smarter Decisions	4
- Android	
- iPhone/iPad	
- Microsoft Windows Phone	
- RIM	
- Symbian	
Conclusion: Making Smart Choices	6
SonicWALL Solutions for Smartphone Security	6



Abstract

Smartphones are everywhere today – equally found in the hands of consumers or the enterprise community. But for all their apparent user-friendliness, smartphones represent a significant threat to corporate data. IT departments need to think long and hard before deciding on the right smartphone platform for their business needs.

Smartphones are among the most important technological developments of our time. Since the advent of the first smartphones in the 1990s, these once cumbersome devices have become immensely powerful and sophisticated tools – not just individual communications devices, but whole computing platforms, capable of running a vast array of personal and business applications.

Today's smartphones rival and even exceed high-end laptops in their feature sets and capabilities. Powerful processors and extensive storage capabilities make them ideally suited to many kinds of computing tasks. Equipped with multiple radio sources and network protocols, they can connect to almost any kind of network on either a managed or an ad-hoc basis. Motion sensors and GPS chips give them superlative navigational capabilities. And increasingly, they are designed to be extremely easy to use, with advanced user interfaces and high-quality displays making them viable alternatives to bigger, heavier laptops.

Such functionality and design has made them extremely popular with users, especially in the last 18 months. Widely available at comparatively low cost, they have captured the imagination of consumer and business users alike at an extraordinary rate. In 2010, analyst firm Gartner estimated that around 297 million smartphones were sold worldwide, representing growth of 72 percent since 2009 and accounting for nearly 19 percent of all mobile phone sales.¹

The User Revolution

Such ubiquity is driving many changes in user behaviour, not least in the enterprise, where users are discovering that they are more than adequate replacements for their bulky, energy-inefficient corporate laptops. Many key business applications such as email are routinely available on smartphones, with some devices, such as RIM® Blackberry, designed primarily as a business email tool. New kinds of mobile devices, such as tablets (essentially large smartphones, with many or all of the communications and networking features built in) have bigger screens and are thus more suitable for reading (and to some extent generating) large volumes of document- or spreadsheet-based content.

Somewhat inevitably, then, business users now view their smartphones and tablets not just as adjuncts to their other computing tools, but as primary devices in their own right – devices that are easier to carry around, use less power and which fulfil a variety of other consumer-focused functions, such as gaming and personal banking. Increasingly, it is the users themselves rather than their IT departments who are dictating which smartphones are right for their business needs. According to industry analyst IDC, so-called individual-liable smartphones (those that users purchase outside formal company policy but use in some capacity for work or attach to corporate networks) will sell faster than any other smartphone segment by 2014, accounting for more than 20 percent of all smart mobile devices². IT departments still have a big role to play in the selection and management of devices within the organisation – but whether they like it or not, they are no longer making all the decisions.

¹ Gartner report: "Competitive Landscape: Mobile Devices, Worldwide, 4Q10 and 2010", February 2011

² IDC report: "Worldwide Business Use Smartphone 2010–2014 Forecast and Analysis", September 2010

Trends like these create significant challenges for IT managers. Security risks, in particular, are a major concern to IT departments accustomed to having full control over access to and usage of business users' laptops. Smartphones are much easier to lose than bigger devices, creating an instant risk to data integrity. They are often much harder to secure, simply because they have more access points; as well as Wi-Fi and Ethernet capabilities, they are also routinely equipped with 3G/4G and Bluetooth® radios, USB ports, SIM card sockets and cameras. At least as worryingly for security professionals, is that smartphones are equipped with a widely varying array of operating systems, each with its own operational models and security issues and often available in several different versions across device manufacturers.

Risk/Reward: A Complex Equation

Perhaps the biggest threat is from users themselves, who are increasingly using their smartphones with scant regard for IT policies; for example, playing games or checking personal webmail while connected to corporate networks. Increasingly, smartphone usage is placing great pressure on corporate network resources, too, especially when users consume high-bandwidth content such as video. More worryingly for already overburdened IT managers, users can often install untested third-party applications (which may present serious security risks in their own right) from app stores without IT having any way to prevent them doing so. According to one study by IDC, people downloaded 10.9 billion mobile apps in 2010 (a figure it thinks will increase to nearly 76.9 billion by 2014³), each a potential threat to corporate security.

Unsurprisingly, malware authors are already exploiting weaknesses in the open app store model, attracted by the increasingly fertile ground for mischief that it represents. Security vendor McAfee® estimates that the number of pieces of mobile malware grew by 46 percent in 2010, many of them on Nokia® Symbian and Google® Android™ platforms⁴. As the number of smart mobile devices grows, McAfee expects cybercriminals to use botnet infections to target mobile devices, as well as more traditional targets such as PCs and laptops.

The combination of these factors presents IT departments with a serious dilemma. On one hand, smartphones are simply too powerful and useful for businesses to ignore, empowering users in completely new ways and enabling them to work far more flexibly and productively. On the other hand, they are also difficult to deploy securely and they add to substantial existing pressure on technology budgets and resources. Getting this balance between reward and risk right is a familiar problem for IT managers. Security must be seen to be enabling the business, rather than holding it back from the rewards many of these new devices offer. However, smartphones present them with new challenges. Not least of these is the risk that the IT department may be actually harming, rather than enabling the business by imposing overly restrictive security policies. In order for organisations to obtain maximum benefit from the smartphone phenomenon, they need to think about how much access they can give to the workforce, not how little. That in turn means making some important decisions about where and how the different smartphone platforms really need securing.

³ IDC report: "Worldwide and U.S. Mobile Applications, Storefronts, and Developer 2010–2014 Forecast and Year-End 2010 Vendor Shares: The "Appification" of Everything", December 2010

⁴ McAfee publication: "Threats Report: Fourth Quarter 2010", February 2011

Making Smarter Decisions

Choosing a smartphone platform that is safe, easy to configure and manage, and that is flexible enough to meet the needs of employees and senior executives sounds easy on paper. In practice, however, it is one of the biggest challenges facing IT managers in 2011.

IT professionals have many factors to consider when assessing smartphone platforms for deployment within the enterprise. As well as the physical device attributes already mentioned, they must also consider the kinds of threats posed by security failures. In particular, lost or stolen phones present a clear risk to integrity of data held on them, which may be of a highly sensitive and/or personal nature. Malware (including spyware and surveillance software) presents various (and usually serious) risks, depending on the platform in question.

To be certain that devices are safe, IT departments must design security policies that are inevitably a complex blend of technology and policy. Some aspects of these systems, such as mandatory reporting of lost or stolen phones, are largely device-independent and are thus relatively straightforward for organisations to enforce. But others, such as varied access levels depending on device type or control and optimisation of smartphone traffic across Wi-Fi networks, clearly depend on more sophisticated technical insight.

Most analysts agree that enterprises should be able to enforce several basic security features on any smartphone, including mandatory passwords, over-the-air device wiping capabilities and data encryption on the device itself. In practice, the choice of the smartphone platform itself will determine the effectiveness of the overall policy. Not all smartphones are equal, and some vendors make it harder than others to enforce rigorous security protocols and policies.

Android

Google's Android operating system for smartphones has been a big hit with the handset vendor community, attracted by the completely open-source nature of the operating system. Such has been its popularity that Gartner thinks that Android will be one of the two dominant smartphone platforms in the next few years, alongside Symbian, accounting for nearly 30 percent market share by 2014 – a figure that some see as conservative in light of the platform's explosive growth in 2010, estimated by Gartner to be 889 percent. Android already accounted for 22.7 percent of the global total in 2010, according to Gartner and Android sales overtook Symbian for the first time in the fourth quarter of 2010. Although seen initially as a consumer platform (with the added benefit of a less restrictive and more flexible apps model than the iPhone), Google has continually improved security support with successive releases of the operating system. This trend will lead to the inclusion of whole-device encryption in 2011. Google has also added other security features, such as remote wipe and upgraded password policy enforcement, adding to Android's appeal to the business community.

iPhone/iPad

Few pieces of technology have garnered as much attention as the iPhone. It remains the smartphone of choice for design-conscious users in its target markets. To date, however, enterprises have not all shared the public's enthusiasm for Apple's iconic device. While Apple cites the closed, tightly controlled iOS ecosystem as a security benefit, many IT managers dislike the fact that applications can only be distributed, installed and backed up via Apple's own app store and iTunes. This presents a problem for organisations wishing to maintain control over the way they deploy their own or trusted third-party applications. In addition, the widespread availability of so-called jailbreak software has allowed users to completely bypass the iPhone's built-in security features and install a wide range of unauthorised and unsigned applications.

Apple has made some effort to become friendlier to enterprise iPhone customers, in particular by supplying VPN capability as standard, enabling access to some features of Microsoft® Exchange and including remote-wipe and automatic device-erasing features. Yet despite the improved remote management APIs in

iOS4, there is still no centralised management facility available from Apple and no whole-device encryption, both deal-breakers for many enterprise customers.

Microsoft Windows Phone

The latest version of Microsoft's mobile device operating system, Windows® Phone 7, attracted a great deal of attention following its launch in 2010. Long criticised for the performance and usability of its mobile operating systems, the company's latest version improves many aspects of the mobile Windows experience, in particular security access features and integration with back-office Microsoft applications that make it a powerful tool for accessing corporate data on the move. Like Apple, however, Microsoft has yet to provide a central console for large-scale management of devices, which limits options for security-conscious IT managers. It is also exclusively dependent on its own version of Apple's App Store – Windows Phone Marketplace – for installation and distribution of applications, diminishing its appeal to the enterprise customer wishing to deploy apps and data in a carefully controlled manner. Despite many positive reviews, the analyst community is not yet convinced of the viability of Microsoft's smartphone platform in the longer term. In September 2010, Gartner predicted that Windows Phone would account for only 5.2 percent of the market in 2011, up from 4.7 percent in 2010⁵, later estimating that it took only 4.2 percent of sales in 2010. Other analysts are slightly more bullish, however, with IDC in particular citing faster than expected growth in the number of Windows Phone apps and a strong developer ecosystem as reasons for optimism⁶. As previously cited, the recent announcement with Nokia may help push Windows into the spotlight.

RIM

While devices such as the iPhone are trying to make the transformation from consumer to business devices, RIM is attempting to make exactly the opposite transition. Long favoured by corporate IT departments for its focus on providing superlative email facilities, RIM's devices have historically not enjoyed the same degree of user evangelism as their more glamorous contemporaries. Apps, in particular, were late arrivals. In February 2011, there were still fewer than 20,000 Blackberry apps in RIM's app store, a small fraction of the number offered by iPhone and Android developers. Blackberry's browser and interface, too, lack the usability of its main competitors. With 16 percent of global sales in 2010, however, RIM is clearly still a force to be reckoned with, especially in corporate markets where its ubiquitous email platform, robust hardware and excellent battery life all appeal to business users. Perhaps its biggest asset is the Blackberry Enterprise Server, which gives enterprises advanced central device management and control of security over the air, a feature unique to date among smartphone vendors. However, as more vendors enter the email fray, many corporate are now seeing the Blackberry Enterprise Server as one of the more expensive options in the field.

Symbian

Nokia's Symbian operating system remains the world's most widely used smartphone platform. While other more glamorous players have largely stolen the media limelight, Symbian comfortably leads the pack in terms of sales. In 2010, 37.6 percent of global smartphone sales (111.6 million units) were Symbian devices, according to Gartner. Because of its global distribution, comparatively low-cost hardware and mature

⁵ Gartner report: "Forecast: Mobile Communications Devices by Open Operating System, 2007-2014", September 2010

⁶ IDC research note by Al Hilwa, December 19 2010

software platform, Symbian has been a hit with many consumers and businesses since its launch, but its reputation in the enterprise market has diminished as more business-focused devices such as RIM's Blackberry have continued to flourish. Symbian's popularity has occasionally made it a target for malware authors, although the Symbian security model makes it very difficult for unsigned software to cause damage to phones or data, even if installation is authorised by the user. Many security features are enabled on Symbian devices (including on-device encryption), while many others can be capably managed by third-party software both on the device and over the air.

Despite its sales figures and generally reliable performance, Symbian has not captured public imagination in developed markets in recent years, creating opportunities for other vendors to chip away at its market share. The most notable of these vendors is Android, whose tremendous growth in 2010 hit Symbian harder than any other platform. In early 2011, Nokia announced a partnership with Microsoft aimed at reversing this trend, which will put the Windows Phone 7 operating system (see below) on high-end Nokia smartphones, offering an additional platform for the IT managers of Nokia customers to support and secure.

Conclusion: Making Smart Choices

Smartphones are an inescapable and largely beneficial element of the modern corporate computing landscape. However, amid the noise about their portability and utility, it is easy to lose track of the fact that every smartphone presents a potential risk to the enterprise. While diligent IT departments will quickly identify the shortcomings of individual devices and platforms, they may struggle to choose a platform vendor capable of meeting all of their stringent security requirements. As this paper's brief overview shows, no single platform excels in all aspects of security; today, most platform vendors place considerably more focus on user-friendliness and flexibility than on adherence to corporate security protocols.

That may change as the platforms develop, with Android and Windows Phone especially well placed to cater to the growing security needs of the corporate marketplace. For the time being, however, business customers need to work with expert third parties to protect their corporate data and networks fully from the many threats that smartphones potentially represent. In particular, they need to choose products and technologies that address the very specific challenges that smartphones present. These challenges are quite different from those that they face elsewhere on their corporate networks. Smartphones have unique potential to make our working lives more productive, but they also have unique potential to cause havoc. Today's smartest IT professionals will look not just to the platform vendors to ensure a peaceful and productive smartphone future, but to the security community too.

SonicWALL Solutions for Smartphone Security

The SonicWALL® Clean VPN™ solution unites SSL VPN and Next-Generation Firewall technologies to enforce granular application-layer access policies while comprehensively inspecting all traffic at the gateway, all the while correlating event information to streamline and enhance security efficiencies. SonicWALL has strategically positioned itself as an industry leader in pioneering Clean VPN technology solutions for organizations of all sizes by enabling the managed integration of its award-winning Secure Remote Access, Network Security Appliance and Global Management System product lines.

SonicWALL offers a comprehensive secure access solution for smartphones. The integrated Clean VPN solution offers an easy-to-deploy and easy-to-manage universal approach for smartphone security. SonicWALL Aventail® WorkPlace™ delivers a policy-driven, device-optimized Web portal that provides easy access to Web-based (including Flash and JavaScript) and client/server applications and critical network resources from an extensive range of smartphone platforms, including Windows Mobile, Apple iPhone, Google Android and Symbian smartphones, as well as DoCoMo iMode devices and WAP-enabled devices.

In addition, SonicWALL Aventail Connect Mobile™, in combination with SonicWALL Aventail E-Class Secure Remote Access (SRA) appliances, provide the most robust remote access solution for Windows Mobile and Android smartphones with "in-office" access optimized for the device, combining a seamless network experience for users, along with a single, centrally managed gateway for mobile access control.

SonicWALL Aventail Session Persistence enables sessions to persist from network to network without the need to re-establish authentication or re-launch a network session. SonicWALL Aventail SSL VPN solutions provide secure ActiveSynch® support for access to Exchange email, contact and calendar services from Apple, Android and Symbian smartphone devices. Advanced SonicWALL Device Watermarking and Device Identification technologies allows administrators to revoke the certificate of a lost or stolen Apple iPhone, iPad, Google Android or Symbian smartphone immediately, or block access from an unauthorized device.



SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124 T +1 408.745.9600 F +1 408.745.9300 www.sonicwall.com

©2011 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. 03/2011