



# 10 Best Practices: Controlling Smartphone Access to Corporate Networks

*A universal, platform-agnostic approach to security best practices, which treats all smartphones as uncontrolled endpoints.*

## CONTENTS

|                                                  |   |
|--------------------------------------------------|---|
| Why Consumer Smartphones Matter to Your Business | 2 |
| The Impact of Smartphones on Network Security    | 3 |
| Best Practices for Smartphone Security           | 4 |
| SonicWALL Solutions for Smartphone Security      | 6 |
| Conclusion                                       | 7 |



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

## Executive Summary

The “Consumerization of IT” has led to the proliferation of personal smartphone devices used as corporate network endpoints. However, upon granting users allowance to use smartphones, companies must contend with related problems, ranging from uncontrolled bandwidth consumption to exposing new conduits for malware attack and data leakage. The growing array of platforms, as well as the growing influence of consumer decision making in corporate smartphone deployments, demands a universal, platform-agnostic approach to security best practices, which treats all smartphones as uncontrolled endpoints. Organizations can implement these practices using currently available technologies, such as SSL VPNs and Next-Generation Firewalls with Application Intelligence and Control.

# Why Consumer Smartphones Matter to Your Business

## **The increasing impact of consumerization**

The “Consumerization of IT” is an industry-accepted idiom introduced by Gartner Inc., who reports that the majority of new technologies enterprises currently adopt for their information systems will have roots in consumer applications.<sup>i</sup> At the same time, because employees work everywhere at any time, and need constant access to key corporate information, they rely upon the same smartphone technology they use in their personal lives to extend their workday and increase efficiency. However, these corporate end users do not allow IT to dictate what smartphone platform they can use (e.g., RIM<sup>®</sup> BlackBerry), or force them to carry one IT-managed smartphone for work and another consumer device for personal use. Typically, IT initially makes exceptions allowing consumer smartphone use by a few select executive employees, often followed by internal engineers and IT technicians, and subsequently, the wider base of employees will demand to use them as well.

Additionally, with an ever-increasing percentage of the workforce having grown up with the Web and cell phones, more workers feel entitled to greater freedom in selecting their business computing devices, and smartphones are their devices of choice. More than a third of consumers in Western Europe will access the Internet using their mobile phones by 2014.<sup>ii</sup> Eighty-five percent of Americans age 15-18 own a mobile phone.<sup>iii</sup> Those now joining the workforce tend to believe that the technology they have at home is better than the one they have at work.<sup>iv</sup> Among “millennials,” sixty-nine percent will use whatever application, device or technology they want, regardless of source or corporate IT policies; less than half will stick to company-issued devices; and a greater percentage compared with older employees will regularly store corporate data on personal smartphones.<sup>v</sup> This trend will only increase over time.

The power of users now rules the day. IT has effectively lost its ability to constrain the choice of smartphone access in a corporate setting. Further vexing IT administrators is that the scope of the issue continues to expand as new categories of devices are introduced to the corporate network, including devices such as the Apple<sup>®</sup> iPhone<sup>®</sup> and iPad<sup>™</sup>.

## **Beyond the tipping point**

The ubiquitous acceptance of smartphones as a business tool has reached its tipping point. Analysts forecasted smartphone sales of 2.5 billion units by 2015, with compound annual growth rates of twenty-six percent in Asia Pacific (twenty-nine percent in China alone); twenty-three percent in North America and thirty-three percent in South America; twenty percent in Western Europe, twenty-five percent in Eastern Europe, and twenty-one percent in the Middle East and Africa.<sup>vi</sup> Nearly half of U.S. consumers access the Internet with their phones,<sup>vii</sup> and one in three U.S. information workers uses a personal mobile phone for work.<sup>viii</sup>

Going forward, analysts forecast that mobile phones will overtake PCs as the most common Web access devices worldwide by 2013, with the combined installed base of smartphones and browser-equipped enhanced phones surpassing over 1.82 billion units. Moreover, by 2014, more than 3 billion will be able to conduct transactions via mobile or Internet technology.<sup>ix</sup>

### **A shift in silicon**

The primary driving factors for technology research and development today are no longer business, industry or the military, but consumers. According to Intel, consumers are the number one users of semiconductors, having surpassed IT and government in 2004<sup>x</sup>. Gartner has stated that consumer markets will drive much of the industry's underlying research and development, rather than the military and business markets.<sup>xi</sup>

As a result, end users look less to corporate IT as a source for technical leadership, but rather to consumer-oriented vendors that cater to their own personal needs. Armed with the latest cutting-edge technology at their disposal, these corporate "prosumers" are no longer willing to be passive recipients of IT allocations.

### **A moving target**

Face the facts: there will be many rapid changes in smartphone platforms, beyond the control of corporate IT. Administrators must deal with multiple operating system platforms, including operating system platforms, including Apple iOS, Google<sup>®</sup> Android, Nokia<sup>®</sup> Symbian and Microsoft<sup>®</sup> Windows Mobile, with an additional potential for new providers from emerging technology powerhouses such as China. As a result, significant IT investment in securing any particular consumer smartphone platform is practically untenable over time.

Additionally, IT must have an agnostic approach to smartphone platforms to support multiple platforms for their users, as well as provide contingency for access continuity. For example, BlackBerry users in certain countries recently faced threatened service outages that could have required them to switch to a different platform.<sup>xii</sup> Subsequently, to minimize risk of regional loss-of-service, a global business cannot depend solely upon the viability of a single smartphone vendor's platform, but instead, must deploy smartphone solutions that are able to facilitate multiple platforms. This potentially undermines any IT controls gained from earlier deployments of BlackBerry Enterprise Server (BES) environments.

The burden of juggling support for multiple smartphone platforms can also take IT resources away from securing other aspects of the network. Ultimately, new business technology should enhance employee productivity, not overwhelm it. Organizations must bear in mind the impact that individually supporting and securing multiple smartphone platforms will have upon administrative overhead and total operating costs.

## **The Impact of Smartphones on Network Security**

### **Smartphones are outside of IT control**

Smartphones operate in two worlds: they can connect to the corporate network over wireless, or bypass the network entirely using mobile cellular connections. That means they might download malware from the Web over 4G, and then disseminate it to the network over the corporate WiFi network. Transferring data in and out of the corporate network, smartphones are beyond IT control. It is harder for IT to control what users do with their smartphone devices, and how these devices expose business data to security threats. Even if IT-issued, any endpoint device that can bypass security measures is insecure.

### **Data leakage and loss**

The proliferation of smartphones in corporate environments creates new and wider potential for data loss and leakage, whether by theft, unauthorized access or unauthorized transmission. Determined professionals can ultimately undermine even "unhackable" smartphone platforms.<sup>xiii</sup> Smartphones may also retain sensitive or proprietary data while connected to the corporate wireless network, and then leak it over unsecured cellular to the Web, and IT has no recourse. In addition, a growing amount of data loss via smartphones originates within the corporate organization. Whether unintentionally, maliciously or driven by profit, a growing amount of sensitive and proprietary data is lost and leaked via smartphone email attachments and FTP uploads.

Locally resident smartphone data is only as secure as its Subscriber Information Module (SIM) card. Users more frequently lose smartphones than computers. Smartphone content is more vulnerable to theft by whoever finds the misplaced device, as network access codes, usernames and passwords are often

unsecured. Even worse, users often pre-program this sensitive information into the handset for automatic log-on. In addition, thieves can thwart attempts by IT to wipe data remotely by simply by removing the SIM.<sup>xiv</sup>

The widespread practice of “jailbreaking,” or opening a phone to customize its features or functionality (such as to overcome restrictions on alternate mobile service carrier networks), also poses a serious security threat. For example, jailbreakers using SSH to enable full access to their smartphones often overlook updating their root passwords, making them accessible to outside attack. Additionally, jailbroken phones often void smartphone service agreements, and jailbroken systems often go untested in product update development.<sup>xv</sup> Moreover, jailbreakers often resell these compromised devices. According to one report, jailbreaking removes eighty-percent of the iPhone’s security precautions.<sup>xvi</sup> Another study received data from approximately 4.0 million jailbroken devices; about 1.5 million of those, had used a pirated application.<sup>xvii</sup>

A smartphone that can access the network via a corporate wireless access point represents the same kind of threat as any other endpoint. The problem is only different in that a phone is less likely to be running security software. A somewhat uncommon threat is the possible compromise of a phone via its Bluetooth connection. This requires physical proximity and a lot of specific knowledge. However, if the ultimate target is a larger network, this may be worth the effort for a perpetrator.

### **Malware infection**

As their numbers increase, smartphones become a more lucrative target for criminal attacks. The same threats that plague traditional computer operating systems can affect smartphones, disseminated in emails, social media sites, games, screen savers, instant messages, slide shows, or in some cases by shady URL-shortening services that make bogus, redirecting links more difficult to identify. Smartphones can magnify malware distribution by spam, phishing, pharming and pretexting. Because smartphones are a more intimate communications channel than a computer, users are more likely to interact with files masquerading as personal communications. Likewise, users cannot as easily detect cues that a Web site is a false front on a handset with a small screen. Again, the infection may not be apparent even after perpetration, and propagate via smartphone across corporate IP networks.

### **Bandwidth overconsumption**

The preponderance of interactive Web 2.0 and streaming media traffic over smartphones can potentially affect corporate wireless network throughput. Some of these applications, such as streaming video applications, constantly evolve to avoid control. In addition, like any Web-facing endpoint device running applications over the network, smartphones present a potential channel for forced denial-of-service attacks.

## **Best Practices for Smartphone Security**

### **Update security policy to include smartphones**

While high-security environments, such as banks or certain governmental agencies, will continue to mandate specifically allocated smartphones, this will be increasingly difficult for these and other organizations as the consumerization continues to grow in importance as a primary driver for smartphone adoption. Today, organizations will find strategic value and tactical efficiency in setting universal policy that is agnostic towards specific vendor platforms. In addition, while IT may find some policies difficult to enforce on personally owned devices (e.g., having users set strong passwords to access their devices, requiring smartphone anti-virus and anti-malware software installation when viable, requiring lost or stolen smartphones that connect to the network to be reported to IT immediately, etc.), such policies nonetheless should be defined and communicated.

### **Treat all smartphones as uncontrolled endpoints**

Due to their inherent mobility and vulnerabilities, IT should treat smartphones as uncontrolled endpoints, whether or not they are company-issued. Smartphones can get lost, stolen or compromised. IT cannot always trust users to be the person they claim to be. Device identification technology uses serial number information to allow organizations to chain a specific smartphone to a specific user, effectively providing a watermark for the device, and thus enabling IT to disable access to corporate resources and if needed remotely disable the device and erase sensitive data if lost or stolen.

### **Establish SSL VPN access to corporate resources**

Smartphone access to business resources over the Web is a lot like e-commerce. To keep it safe, organizations should apply the methods of successful e-business innovators. To secure online transactions, they apply technologies like Secure Sockets Layer Virtual Private Networking (SSL VPN). SSL VPN can provide a secure universal, portal-based method for smartphone access to network resources, regardless of platform type, and with minimal demand on IT support. For example, instead of setting up, administering and updating separate security solutions for Apple iOS, Google Android, Nokia Symbian and Microsoft Windows Mobile smartphone operating systems, IT could deploy a centralized SSL VPN portal that could provide authenticated and encrypted Web-based access to network resources agnostically, regardless of the smartphone platforms.

### **Vary level of access based on interrogation of device.**

IT should utilize remote access technologies capable of interrogating remote devices to determine what level of access is appropriate based on device and user identity. A single level of trust should not be granted to all connections. Levels of trust should be based on knowing the device type, what is running on the device, whether the device is corporately allocated, etc. Once the security posture has been determined, appropriate levels of security policy should be assigned to that connection.

### **Comprehensively scan all smartphone traffic**

To protect network resources, IT should deploy a Next-Generation Firewall to conduct deep packet inspection that can comprehensively scan all smartphone traffic—whether over internal WiFi, or going in or out of the network over SSL VPN—and protects against malware, intrusions, Trojans and viruses.

### **Control data-in-flight**

IT should be capable of inspecting outbound traffic for data leakage, even if that traffic is encrypted. At the same time, IT should scan all data-in-flight for malware, and prevent internally launched outbound botnet attacks that can damage corporate reputation and get business-critical email servers blacklisted.

### **Maximize firewall throughput to eliminate latency**

When smartphones are connected to the corporate network, in order to minimize impact upon latency-sensitive applications, such as video conferencing and voice over IP (VoIP), the Next-Generation Firewall platform must be capable of comprehensively scanning smartphone traffic in real-time. IT can obtain such performance capability in solutions that integrate reassembly-free deep packet inspection methods with high-speed multi-core processor architecture.

### **Establish controls over smartphone application traffic**

As primarily a Web-enabled device, smartphones users can access applications such as social media and streaming video. IT should establish control over these applications, just like with other devices when connected directly to the corporate network. Application Intelligence and Control technology can extend firewall functionality to identify, categorize, control and report upon application usage over the corporate network from these devices.

### **Establish smartphone wireless access security**

Analysts expect ninety-percent of smartphones to have WiFi functionality by 2014.<sup>xviii</sup> Security for wireless networks has to be at least on par with wired networks running deep packet inspection. IT should apply both WPA2 and Application Intelligence and Control to traffic from users connected to the corporate network over WiFi. To be as secure as wired networks, WLANs also need other security features, such as deep packet inspection (DPI), to scrub traffic using an array of intrusion prevention, anti-virus and anti-spyware technology.

### **Manage smartphone traffic bandwidth**

Organizations need to control converged voice-and-data communications enabled by smartphones when directly connected to the corporate network, while at the same time continuing to optimize quality of service and bandwidth management, as well as prioritization on a per-application and per-user basis. Application-intelligent bandwidth management can both dedicate throughput to latency-sensitive smartphone applications such as VoIP, as well as limit bandwidth-consuming traffic, such as YouTube.

## **SonicWALL Solutions for Smartphone Security**

The SonicWALL® Clean VPN™ solution unites SSL VPN and Next-Generation Firewall technologies to simultaneously enforce granular application-layer access policies, comprehensively inspect all traffic at the gateway, and correlate 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 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 SSL VPN solutions provide secure ActiveSync® support for access to Exchange email, contact and calendar services from Apple, Android and Symbian smartphone devices. 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 Device Identification provides administrators with the ability to chain a specific smartphone to a specific user, so in the event that phone is lost or stolen the administrator can quickly revoke corporate access. SonicWALL Application Intelligence and Control allows custom access controls based upon user, application, schedule, or IP subnet level. Its comprehensive policy capabilities include restricting transfer of specific files and documents, blocking email attachments using user-configurable criteria, customizing application control, and denying internal and external Web access based on various user-configurable options.

The patented SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI) technology (U.S. Patent 7,310,815D-A) combines a single scanning engine with a high speed, multi-core, parallel hardware architecture to enable simultaneous, multi-threat scanning and analysis at wire speed, which is essential for high-bandwidth networks. By integrating advanced networking and remote access technologies, SonicWALL verifies and defends the security of traditional and mobile wireless networks, users and applications—and their endpoint devices—while scanning and disinfecting the entire data stream across platforms and perimeters.

SonicWALL Clean Wireless™ delivers the dual protection—combining high-speed secure wireless and with high-performance full deep packet inspection—that is required to secure the wireless connection, and inspect and encrypt the traffic flowing over the wireless network. By integrating SonicPoint-N Dual-Band™ Series of access points with SonicWALL network security appliances over a central point of management, SonicWALL Clean Wireless supports and enforces one set of security policies over both wired and wireless networks.

## Conclusions

In regards to personal smartphone usage in corporate environments, the Consumerization of IT has reached an irrevocable tipping point. While mandating and allocating corporate-issued devices will continue, end users will increasingly demand access to network resources from personal consumer smartphone devices. While riding this tide does offer potential business benefits, it comes with inherent risks. SonicWALL solutions, including Next-Generation Firewall, Clean VPN, Clean Wireless, and Application Intelligence and Control, can help organizations easily implement best practices to secure smartphone use in corporate network environments



**SonicWALL, Inc.** 2001 Logic Drive, San Jose, CA 95124 T +1 408.745.9600 F +1 408.745.9300 [www.sonicwall.com](http://www.sonicwall.com)

©2010 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. Specifications and descriptions subject to change without notice. 10/10 SW#

- 
- <sup>i</sup> “Gartner Says Consumerization Will Be Most Significant Trend Affecting IT During Next 10 Years,” Gartner Inc., October 20, 2005
- <sup>ii</sup> “Western European Mobile Forecast, 2009 To 2014,” Forrester Research, August 31, 2009
- <sup>iii</sup> Media in the Lives of 8 to 18 Year Olds, The Kaiser Foundation, January 2010
- <sup>iv</sup> “The State of Workforce Technology Adoption: US Benchmark 2009,” Forrester Research, Inc., November 11, 2009
- <sup>v</sup> “Millennial Workforce: IT Risk or Benefit?,” Symantec, March 2008
- <sup>vi</sup> “Worldwide Smartphone Sales Forecast to 2015,” Coda Research Consultancy, May 2010
- <sup>vii</sup> “The Mobile Internet Report Setup,” Morgan Stanley, December 2009
- <sup>viii</sup> “The State of Workforce Technology Adoption: US Benchmark 2009,” Forrester Research, Inc., November 11, 2009
- <sup>ix</sup> Gartner: Mobile To Outpace Desktop Web By 2013,” Media Post Communications, January 13, 2010
- <sup>x</sup> “For future of enterprise computing, watch consumers,” CNET News, November 14, 2007
- <sup>xi</sup> “Gartner Says Consumerization Will Be Most Significant Trend Affecting IT During Next 10 Years,” Gartner Inc., October 20, 2005
- <sup>xii</sup> “Emirates to Cut Data Services of BlackBerry,” New York Times, August 1, 2010
- <sup>xiii</sup> “‘Unhackable’ Android phone can be hacked,” Network World, July 29 2010
- <sup>xiv</sup> “5 Things You Need to Know About Smartphone Security,” CIO Magazine , September 8, 2009
- <sup>xv</sup> “Jailbreaking Your iPhone: The Pros and Cons,” Macworld, August 6, 2010
- <sup>xvi</sup> “Apple patching critical SMS vulnerability in iPhone OS,” Ars Technica, July 3, 2009
- <sup>xvii</sup> “Piracy in the App Store (from 360iDev),” Pinch Media, October 12, 2009
- <sup>xviii</sup> “Survey: Wi-Fi becoming smartphone must-have,” CNET News, April 1, 2009