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

Executive Summary

The “Consumerization of IT” has led to the proliferation of personal smartphone devices used as corporate network endpoints. However, when allowing the use of consumer 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 consumers 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 or Unified Threat Management 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.[i] At the same time, because employees now 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, IT can no longer force users to carry one IT-managed smartphone (e.g., RIM® BlackBerry) for work and another consumer device for personal use.

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.[ii] Eighty-five percent of Americans age 15-18 own a mobile phone.[iii] Those now joining the workforce tend to believe that the technology they have at home is better than the one they have at work.[iv] 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. Moreover, a greater percentage compared with older employees will regularly store corporate data on personal smartphones.[v] 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® iPhone® and iPad™.

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, 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.[vi] Nearly half of U.S. consumers access the Internet with their phones,[vii] and one in three U.S. information workers uses a personal mobile phone for work.[viii]

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.[ix]

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[x]. Gartner has stated that consumer markets will drive much of the industry's underlying research and development, rather than the military and business markets.[xi]

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 Apple® iOS, Google® Android, Nokia® Symbian and Microsoft® 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.

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.[xii] 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. The need for platform flexibility could potentially undermine IT controls gained from mandated deployments of single-vendor platforms, such as BlackBerry Enterprise Server (BES).

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 Wi-Fi 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 issues them, 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.[xiii] Smartphones may also retain sensitive or proprietary data while connected to the corporate wireless network, 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.[xiv]

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 Secure Shell (SSH) applications 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.[xv] Moreover, jailbreakers often resell these compromised devices. According to one report, jailbreaking removes eighty-percent of the iPhone’s security precautions.[xvi] Another study received data from approximately 4 million jailbroken devices; about 1.5 million of those had used a pirated application.[xvii]

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 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, which 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 sheer volume of interactive Web 2.0 and streaming media traffic over smartphones can 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

Best practices demand that IT enforce sound smartphone policy with proven technology. IT should define, document and communicate smartphone use policy, and couple that policy with the deployment of corresponding enforcement solutions. Examples of documented IT policy include requiring users to set strong passwords on their smartphones (valuable in cases of lost devices, etc.) and report lost or stolen smartphones to IT immediately. Examples of enforcement solutions include security technologies that can recognize when solicited connections are originating from smartphones and provide differentiated access policies based on type of device and user authentication. The following best practices include approaches for both policy and technology.

1. Establish SSL VPN access to corporate resources

Instead of setting up, administering and updating separate security solutions for separate smartphone operating systems (e.g., Apple iOS, Google Android, Nokia Symbian and Microsoft Windows Mobile), IT could deploy a centralized Secure Sockets Layer Virtual Private Networking (SSL VPN) portal. An SSL VPN portal can provide authenticated and encrypted Web-based access to network resources agnostically, regardless of the smartphone operating systems using reverse proxy, and minimize demand on IT support. Moreover, when integrated with firewall technology to form a “clean VPN” solution, an SSL VPN, establishing an authorized Web portal, can enable tight controls on data management while providing superior security and malware protection for the corporate network.

2. Vary access levels based on device interrogation

In conjunction with SSL VPN portal access, 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. An effective secure remote access solution should not grant a single level of trust to all connections, but vary levels of trust based on knowing the device’s security posture (including device type, what is running on the device, whether the device is corporate-allocated, etc.). Once the security posture has been determined, the solution should assign and enforce appropriate levels of security policy to that connection. By limiting users from accessing and downloading sensitive data, this technology can reduce or eliminate broad data leakage threats, while still providing relevant data to support mobile workers.

3. Require lost or stolen phones be reported immediately

Smartphone policy should require that lost or stolen phones be reported immediately. Due to their inherent mobility and vulnerabilities, IT should treat smartphones as uncontrolled endpoints, whether or not they are company-issued. 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 lost or stolen, remotely disable the device and erase sensitive data.

4. Comprehensively scan all smartphone traffic

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

5. 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. Full-featured Next-Generation Firewalls and UTM Firewalls can provide those protections.

6. 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 or UTM Firewall platform must be capable of comprehensively optimizing business-relevant smartphone traffic in real-time. IT can obtain such performance capability in solutions that integrate reassembly-free deep packet inspection methods with a high-speed multi-core processor architecture.

7. Establish controls over smartphone application traffic

As primarily a Web-enabled device, smartphones enable access to applications such as social media and streaming video. To enforce adherence to corporate policy, 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.

8. Establish smartphone wireless access security

Analysts expect ninety-percent of smartphones to have Wi-Fi functionality by 2014.[xviii] Security for wireless local area networks (WLANs) has to be at least on par with wired networks running deep packet inspection (DPI). IT should apply WPA2 as well as 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 DPI, to scrub traffic using an array of intrusion prevention, anti-virus and anti-spyware technology.

9. 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 (QoS) and bandwidth management, as well as prioritization on a per-application and per-user basis. Application-intelligent bandwidth management can dedicate both throughput to latency-sensitive smartphone applications such as VoIP, and limit bandwidth-consuming traffic, such as YouTube.

10. Visualize bandwidth activity

To control the proper use of mobile networks, administrators need tools to view traffic and adjust network policy based on critical observations. This enables administrators to ensure bandwidth for smartphone traffic, while adjusting policy to restrict or block bandwidth-consuming traffic based upon a real-time view of bandwidth utilization, application and user traffic, and other user activity.

SonicWALL Solutions for Smartphone Security

To implement these best practices, IT requires solutions with the capability to enforce them.

SonicWALL Secure Remote Access

SonicWALL® Secure Remote Access (SRA) and SonicWALL Aventail® E-Class SRA solutions deliver easy, policy-driven access to critical network resources from an extensive range of smartphone platforms, including Windows Mobile, Apple iPhone, Google Android and Symbian smartphones.

SonicWALL Aventail WorkPlace™ delivers a policy-driven, device-optimized Web portal that provides easy access to Web-based (including Adobe® Flash® and Oracle® 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 i-mode® devices and WAP-enabled devices.

In addition, SonicWALL Aventail Connect Mobile™, in combination with SonicWALL Aventail E-Class Secure Remote Access (SRA) appliances, provide an exceptionally 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 Microsoft Exchange email, contact and calendar services from Apple, Android and Symbian smartphone devices. SonicWALL Device Identification lets administrators chain a specific smartphone to a specific user, so, in the event that phone is lost or stolen, they can quickly revoke corporate access. In addition, SonicWALL Aventail Advanced End Point Control™ (EPC™) offers advanced endpoint detection and data protection for distributed enterprises, by interrogating endpoint devices to confirm the presence of all supported anti-virus, personal firewall and anti-spyware solutions from leading vendors like McAfee®, Symantec®, Computer Associates®, Sophos®, Kaspersky Lab® and many more.

SonicWALL Clean VPN

The integrated SonicWALL Clean VPN™ solution offers an easy-to-deploy and easy-to-manage universal approach for smartphone security. The SonicWALL Clean VPN solution unites SSL VPN and Next-Generation Firewall or UTM 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. 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 Application Intelligence and Control can maintain granular control over applications, prioritize or throttle bandwidth, and manage Web site access. 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 SonicWALL Application Flow Monitor provides real-time graphs of applications, ingress and egress bandwidth, active Web site connections and user activity. This visualization capability enables administrators to effectively monitor and revise policy based on critical observations

SonicWALL Clean Wireless

SonicWALL Clean Wireless™ delivers dual protection—combining high-speed secure wireless 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™ access points with SonicWALL firewalls over a central point of management, SonicWALL Clean Wireless supports and enforces a unified set of security policies over both wired and wireless networks.

Moreover, the SonicWALL Global Management System (GMS) enables organizations of all sizes to globally manage, monitor, and generate reports on the activity of up to thousands of remote SonicWALL appliances.

Conclusions

The consumerization of personal smartphones in corporate environments 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 SSL VPN, Clean VPN, Next-Generation Firewall, UTM, Clean Wireless, and Application Intelligence, Control and Visualization, can help organizations easily implement best practices to secure smartphone use in corporate network environments

SonicWALL's line-up of dynamic security solutions

NETWORK SECURITY

SECURE REMOTE ACCESS

WEB AND E-MAIL SECURITY

BACKUP AND RECOVERY

POLICY AND MANAGEMENT

SONICWALL®

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

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