WEBROOT®

Cloud-Based Mobile Device Security Streamlines Data Protection

Contents

Brought to you compliments of

WEBROOT®

Executive Summary

As smartphones and tablets have become increasingly sophisticated, the amount and types of data stored on them have increased. Confidential data once stored inside the firewall now resides on mobile devices, but many small and medium businesses have not taken sufficient action to address the risks this presents.

SMB IT staff may believe that only large enterprises are at risk. But according to one report, 40% of attacks have been directed at SMBs, while only 28% have been directed toward large enterprises.[1]

The diversity of device types complicates data protection. Traditional security solutions require a different product for each type of device, each with its own management facility and each with its own command set, increasing IT management complexity and resource requirements.

[1] Small and Midsize Business Guide to Mobile Security, Webroot and Tech Target, 2012

Read this white paper to learn why cloud-based security offers superior protection that meets today's requirements for identifying and preventing access to malicious sites and applications while reducing management complexity and IT staff time and effort. This whitepaper discusses:

- Increased use of mobile devices and the associated risks
- Ways to address security challenges
- Benefits of cloud-based anti-malware solutions

Security Challenges

The rapid adoption of smartphones and tablets has attracted the attention of hackers and other intruders, increasing the risk of data loss for SMBs as well as large enterprises.

The Department of Homeland Security reported a 400% increase in attacks on Android devices between mid-2010 and June 2012.[2] Apple's iOS devices are targeted less frequently, since apps are available only from Apple's App Store, but some malicious apps have slipped through Apple's tests as well.

The reason for these attacks is simple: Mobile devices increasingly contain valuable information. Sales staff with customer and price lists, field service technicians with detailed product information, and health care workers with patient information are all potential targets.

Data resident on mobile devices is not the only target. Users typically store passwords and PINs on their devices to avoid having to enter them for each access point. An attacker who captures a VPN password, for instance, can easily gain access to server-based data that is considered safe inside the corporate firewall.

Attackers can profit from a successful attack and cause financial loss for a business even when the compromised device contains nothing confidential and no valuable passwords. For example, malware can charge Premium SMS messages to a corporate phone number lifted from a phone's contact list. It's not hard to miss a series of $5 to $10 charges scattered through a long cell service log, but these charges can add up.

The bring-your-own-device trend, with employees using their own devices for work purposes, further adds to the challenge of protecting corporate data. One problem is that conventional anti-malware products are designed for a single device type, but it's inevitable that staff members won't all choose the same type of device. The result: IT staff must learn how to maintain and monitor multiple device types while using multiple security products.

User-installed apps represent another major business risk. It's virtually impossible to prevent employees from choosing and installing apps on their personal devices. Attackers create apps that offer a free game or another attractive feature but contain code that compromises device security.

Malware is not the only danger. Data loss due to lost or stolen devices is also a major problem. A 2012 survey conducted by Research Now found that among businesses with up to 50 employees, roughly a quarter had dealt with device loss or theft.[3]

[2] OIG 12-88: DHS Needs to Address Portable Device Security Risks, June 2012

[3] Survey: Mobile Threats are Real and Costly, Research Now/Webroot, 2012

SMBs Slow to Implement Mobile Security

Despite the widely publicized losses resulting from targeted attacks, many SMBs have not taken action to address mobile device security. Research Now found that fewer than half of the enterprises surveyed had implemented a security solution.[4]

Several factors have impeded adoption of appropriate mobile security measures.

First, IT staff may be unaware that employees are transferring confidential information to privately owned devices. Second, with SMB IT staff already supporting in-house desktop systems, mobile laptops and servers, they may believe that implementing a mobile device solution that protects the variety of devices in employees' hands would be too time-consuming, complex and expensive.

Traditional security requires a different product for each type of device: one for Windows-based desktops and laptops, another for conventional servers and yet another for virtualized servers. Each requires its own management console with its own set of commands. Now add in mobile products with two more management facilities, one for Android and one for Apple iOS devices. It's no wonder that IT staff already struggling to deal with on-premises systems are not eager to add mobile devices to their workload.

Traditional mobile security solutions have an additional drawback. They require that staff have hands-on access to install software updates and make policy changes. Scheduling updates for a time when a device will be available in-house adds more complication. At any given time, some devices have been updated while others haven't. The task becomes even more complex and time consuming when the staff must support a mix of device types, each protected by a different security product.

While overburdened IT staff at many SMBs have avoided implementing mobile device security, it's clear that doing so is no longer feasible. The risks are too great. However, with the right security solution, SMBs can implement improved security defenses while streamlining IT management challenges.

Cloud-Based Security Solutions Simplify Management

Reducing IT staff time and effort requires a security solution that supports both Android and Apple iOS mobile devices as well as current in-house systems. Increasingly, SMBs are looking to cloud-based solutions as a way to support all of these systems with reduced management effort and simultaneously provide better protection than traditional products.

Managing via the cloud simplifies labor-intensive tasks. A single management console manages both on-premises and mobile devices, and there is just one set of management commands to learn. Instead of configuring devices one by one, IT staff members enter a single set of commands to a cloud-resident management server.

[4] Ibid, footnote 3

Updates are delivered to all devices simultaneously, so policy changes become effective for all connected devices immediately. Any devices that are out of range of cell service or Wi-Fi — or are shut off — automatically receive the updates upon their next connection to the Internet.

Cloud management offers these benefits:

- Eliminates the need to invest in a management server and management software.
- A single management facility supports all devices.
- Updates are made using a standard Web browser.
- Cloud resources are scalable and redundant.
- Eliminates the need to upgrade an in-house management server when the device population increases or to delay required policy changes because the management server is down.

Cloud-Based Solutions Provide Superior Device Security

Traditional mobile device protection software executes inside each device, monitoring incoming email and webpages as they are received and comparing their contents against a previously downloaded threat signature file. Inspecting and analyzing incoming data requires a large device-resident application and consumes processor resources.

Dealing with today's wide variety of threats requires a significant amount of memory for the application itself and for the threat signature database. Additionally, with traditional products, each database download consumes network bandwidth, processor time and cell service monthly quota. As a result, devices typically update, at most, every few hours.

With their need for periodic updates, traditional security products leave devices vulnerable. According to testing company AV-TEST, 55,000 new malicious programs are detected each day.[5]

Attackers understand that defenses against any new attack type will be created quickly, so any new method is most valuable during the first day it's used. To take maximum advantage, they attack multiple sites as quickly as possible. Devices protected by traditional products remain open to the new attack in the hours until their next update.

In contrast, cloud-based solutions greatly increase mobile protection. Here's how:

First, they offload data inspection to powerful cloud processors that scan the Internet 24 hours a day, searching for malicious websites and device apps. Suspicious websites and apps are evaluated using processors with far more compute power than those found on mobile devices.

When a new website or app is discovered, cloud processors examine it in detail. They check webpages for embedded malware and execute apps in a protected environment to determine what privileges they would request from a mobile device operating system and whether they would perform other actions that would compromise a device.

[5] See Webroot SecureAnywhere Endpoint Security.

Second, information about webpages and apps is stored in the cloud, where storage space is virtually unlimited. As a result, cloud-based solutions can maintain a threat database far larger than any mobile device can support.

Third, cloud-based solutions support a worldwide community of users. As soon as an attack is detected on one user, the attack is analyzed and the cloud-resident threat database is updated.

Fourth, cloud solutions don't require a periodic threat download. Devices check incoming mail, websites and apps against the cloud database. If the cloud has determined that the object contains a threat, it's blocked. Devices are protected as soon as possible after the first appearance of a new threat. There's no need to wait hours until the next threat signature downloads.

Webroot SecureAnywhere Mobile Protection

Webroot's SecureAnywhere Mobile Protection greatly eases the load on IT management staff by supporting both Android and Apple iOS mobile software environments. SecureAnywhere Mobile Protection is part of Webroot's Secure Anywhere Business platform, which also delivers endpoint protection for laptops, desktops, servers and virtualized environments.

Uniform policies govern all devices. When a change is made, it applies to all devices without the need to wait until a mobile device is brought in-house, and there's no need to configure devices one by one. Connected devices are updated immediately over the air, while those without Internet access are updated as soon as they are connected.

SecureAnywhere Endpoint Protection supports Microsoft Windows desktops, laptops and Windows servers, plus virtualized servers supported by VMware, Citrix and Microsoft software. Both SecureAnywhere Mobile Protection and SecureAnywhere Endpoint Protection are managed from the same portal, further reducing management load and complexity.

There's no need for a traditional management application and no capital cost to acquire an in-house management server. Management is done using a standard Web browser to access a cloud-based security service. Staff members do not even have to switch from their favorite browser: SecureAnywhere Mobile Protection supports all popular browsers, including Internet Explorer, Firefox, Chrome, Safari and Opera.

Devices can be managed from anywhere, so an IT staffer with the proper login credentials can connect from home or anywhere to make needed changes. The staffer can make changes to any device or to all devices. If an issue arises that affects all devices, the staffer can make a global policy change.

A single login to the cloud-resident management server is all that's required. There's no need to connect through the firewall to an on-premises management server to update on-premises systems and then connect to another facility to modify mobile devices. One connection and one set of commands is all that is needed.

Management is further simplified by a set of default and preconfigured policy templates. Cloud-based management constantly monitors all devices, generating alerts, notifications, and real-time

ad hoc and scheduled logs. The network monitor tracks and logs all applications that access the network. Alerts can be sent via email or SMS as well as to the management console.

Using the SecureAnywhere Mobile Protection portal, a lost or stolen device can be remotely locked — even if the SIM card has been removed — and located on a map. All data stored on the device can be erased. In cases where a device can't be found but is known to be nearby, a management command can help locate it by signaling the device to emit a loud noise.

In addition, because SecureAnywhere Mobile Protection occupies a very small memory footprint, new devices can be provisioned in a fraction of the time required by traditional products.

SecureAnywhere Mobile Protection provides superior protection while consuming minimal device battery and bandwidth resources, according to industry research.[6] The key differentiator is the Webroot Intelligence Network, which consists of powerful processors and storage resources residing in the cloud. It gathers information by constantly scanning the Internet for malicious objects and gathering information from test labs, customers and information shared by other security vendors.

The Intelligence Network is always up. It consists of multiple data centers spread around the world, each supporting nearby offices and mobile users. In the event that a data center becomes unavailable, others pick up the load.

The Intelligence Network's 100-plus terabytes of threat information identify far more threats than could be included in signature files downloaded to any desktop, laptop or mobile device.

SecureAnywhere Mobile Protection blocks unwanted calls and SMS messages containing links to malicious sites. It prevents Premium SMS calls by analyzing and preventing installation of apps that would make these calls. SecureAnywhere Mobile Protection also protects against phishing attempts by analyzing links found in email and blocking access.

Some competitors' cloud-based products support a single type of mobile device, Android. Webroot SecureAnywhere Mobile Protection and SecureAnywhere Endpoint Protection support all of these systems: desktops, laptops, Android and iOS, as well as conventional and virtualized servers, all from the same management portal.

Other cloud-based products support both Android and iOS devices but require investing in an in-house management system. It's impossible to manage mobile devices when the management server is down or can't be reached for some reason. SecureAnywhere Mobile Protection's cloud-based management solution is redundant and therefore always accessible. An additional advantage of Webroot's solution is that it's scalable, unlike other cloud-based products. There's never a need to invest in a new management server when the device population grows.

Webroot SecureAnywhere Mobile Protection and SecureAnywhere Endpoint Protection represent an effective solution for today's SMB needs, with support for an extensive array of devices using the same integrated management console. The Webroot Intelligence Network provides superior protection against all forms of malware, including zero-day attacks that often elude other solutions.

[6] See AV-TEST and *PC Magazine* tests.