Building a Business Case: Integrated Mobile Security For Small and Midsize Businesses:

table of contents

+ Introduction ................................................................. 2
+ Solutions for SMBs ......................................................... 3
+ Key Features SMBs Should Require for Mobile Security ............ 4
+ Choosing the Right SMB Solution ..................................... 6
+ Conclusion .................................................................... 7
Introduction

Mobility is one of the driving factors for all business and IT initiatives. IDC has characterized it as one of the four pillars of computing’s next dominant platform, along with social media, Big Data and cloud services.\(^1\) Mobility has the potential to dramatically enhance business agility, improve employee productivity and enable major shifts in the way individuals and businesses approach work.

Yet for mobility to fulfill all of this vast potential as a business catalyst, organizations must focus on and successfully address the new security vulnerabilities it creates. Mobility poses specific challenges for small and midsize businesses (SMBs), many of which don’t have any security solutions in place to manage mobile devices and security, and may not even be fully aware of the growing volume and intensity of targeted attacks on mobile devices.

SMBs don’t have the luxury of waiting to implement mobile security solutions. Why?

- **BYOD and the Consumerization of IT:** Like it or not, employees are bringing their own devices to work and using them for both business and personal activities. According to one survey, 80% of employed adults are using a personally owned device for work.\(^2\) These devices are making organizations much more vulnerable to attack, which means they must take steps to ensure that personally owned devices are as secure as every other endpoint device attached to the corporate network. More than 83% of respondents to a recent survey commissioned by Webroot believe that mobile devices create a high security risk within the corporate environment.\(^3\)

- **An Evolving Threat Landscape:** SMBs are more vulnerable in general because cybercriminals assume that smaller organizations have lax security and therefore attack them more often: In 2012, attacks against SMBs have doubled compared with 2011.\(^4\) Cybercriminals are also quite adept at targeting an organization’s most vulnerable weaknesses, making the mobile endpoint an inviting target, particularly in the SMB

---

\(^1\) IDC Predicts 2012 Will Be the Year of Mobile and Cloud Platform Wars as IT Vendors Vie for Leadership While the Industry Redefines Itself, IDC, December 1, 2011

\(^2\) The BYOD security challenge: How scary is the iPad, tablet, smartphone surge? ESET Threat Blog, Feb. 28, 2012

\(^3\) Survey: Mobile Threats Are Real and Costly, Webroot, November 2012

\(^4\) New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity: Majority Have No Policies or Contingency Plans, National Cyber Security Alliance, October 2012
environment, where adequate security safeguards may not be in place. In fact, mobile attacks grew by nearly 20% in 2011 and have increased nearly tenfold since 2009.  

More Vulnerable User Activities: Individuals using smartphones and other personally owned devices tend to engage in activities that increase the risk of attacks on the business – for example, using social media sites to a greater degree or visiting web sites that may increase vulnerabilities, such as gambling or pornography sites. Also, mobile devices are more vulnerable to loss or theft, which could put your business in danger if they can access corporate data. One of the other challenges with smartphones is that they offer real mobility as opposed to just portability: Users tend to keep them on all the time, even when they are not in use, which further increases their vulnerability to attack.

For SMBs, the security threats that come with increased mobility are not only real, but they are growing rapidly and can be quite damaging. One survey shows that a single breach costs an average of $214 for each compromised record, and the average major data breach event costs $7.2 million. That's damaging enough to put most SMBs out of business. Yet 83% of SMBs have no cybersecurity plan, and nearly 60% say they do not have a contingency plan outlining procedures for responding to and reporting data breach losses.

Solutions for SMBs
Fortunately, SMBs have access to security solutions that can address their mobile challenges without doing major damage to their budget. And by deploying a cloud-based solution, any SMB can move quickly to get protection up and running, without having to invest in new infrastructure or hire a team of IT security experts.

So what types of solutions are available for SMBs, and how should IT managers and administrators make the business case for what to adopt?

One class of solution targeted at the large enterprise is mobile device management (MDM), but for most SMBs, these solutions are overkill and many of the available features would not be used. What's more, most MDM solutions don't focus specifically on security and may lack some of the key security features required by SMBs.

---

6 Cost of Data Breach Climbs Higher, Ponemon Institute, March 8, 2011
7 New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity: Majority Have No Policies or Contingency Plans, National Cyber Security Alliance, October 2012
In making the business case for mobile security, SMB administrators and decision-makers should focus on cost-effective solutions that address their core, vital security needs. What’s more, they want to make sure that their solutions are simple to deploy and manage. Finally, SMBs should look for a mobile security solution that is tightly integrated with their endpoint PC and server solution, which will make it much easier to deploy, provision and manage, with the capability to establish, update and enforce consistent protection across all devices.

As noted, another important consideration for SMBs is whether to choose a cloud-based solution versus a premises-based option. There are significant advantages in going with a cloud-based solution:

- Much more flexibility and speed in deploying updates, which is critical in mobile security because the threat landscape is changing so rapidly
- No additional expenses for hardware and software infrastructure
- Far less demands on the IT staff and the ability to leverage the specific security expertise of your cloud supplier
- Ability to quickly provision and consistently apply new security features and policies to all devices as soon as they become available
- Ability to quickly enforce rules and deploy enhanced protection when company policies are violated

Key Features SMBs Should Require for Mobile Security

While there are a plethora of SMB security solutions on the market today, mobility brings special challenges. First off, make sure that whatever solution you are considering is one that specifically targets the unique security challenges of mobile devices.

For example, you want a solution that supports the major mobile operating platforms, such as iOS and Android. It should utilize a lightweight client so that it doesn’t impact user performance. And it must be able to secure and protect your business if a device – any device, company-sanctioned or personally owned – gets lost or stolen. Finally, it should provide protection no matter where or when the device is being used.
Here’s a quick checklist of features to consider in making the business case for adding an extra layer of protection for mobile security:

1. **Management**: Can you manage security for all of your mobile devices and other endpoints from a single console? Does your solution leverage the cloud for management and protection? Does it support all of the platforms users may be bringing with them from the consumer world?

2. **Protection**: Does your solution provide adequate protection for lost or stolen devices – specifically, does it give you the ability to lock, wipe, locate and scream a lost phone? Does it support secure Web browsing, and does it offer advanced anti-malware detection that would enable your organization to remove known and unknown infections before they do harm?

3. **Performance**: Does it deploy lightweight clients for fast scans and efficient battery utilization? Does it use the cloud to minimize impact on network performance, and does it offer simple scalability to enable quick and secure deployment of new smartphones and other devices?

4. **Integration**: Does your mobile security solution seamlessly integrate with your existing solution for other endpoints so that you can apply the same policies, rules, features and enforcement across your entire organization? Can the same support team manage security for your traditional endpoints as well as the newer generation of smaller consumer devices?

As with making any business case, costs are always a critical consideration. This is one of the ways in which deploying a mobile security cloud service will be extremely attractive. Your organization will save significant money up front by not having to purchase additional hardware and software, and it will save over the long term in support, maintenance and upgrade costs. The organization will not have to hire additional IT personnel and will be able to take advantage of the insight and expertise of the cloud supplier as the threat landscape continues to shift, which it certainly will.
The other important consideration in building a business case is risk versus reward. In the case of mobile security, the potential damage to your organization through a breach or malicious attack could be devastating, while the cost of deploying an effective cloud solution is extremely reasonable. In addition, because of the elastic scalability of the right cloud solution – you should be able to add new devices immediately just by loading the client software – your costs and support requirements won’t skyrocket as you add new users.

Choosing the Right SMB Solution

While there are many security solutions that purport to address mobility concerns for SMBs, you want to make sure the solution you choose meets all of the key requirements of the business case you are building. It should:

- Support the shift to BYOD and the consumerization of IT, focusing on the specific challenges of securing mobile devices
- Provide protection that is agile enough to address the current – and future – threat landscape
- Access an intelligent threat detection network that provides real-time protection against new and emerging threats
- Be cloud-based for maximum protection, cost efficiencies, elastic scalability and simplified manageability
- Integrate seamlessly with existing endpoint security, so the same team can manage all devices from a single console

When you consider all of those requirements, the one solution that stands out is Webroot Mobile Protection, which is a cloud-based offering designed specifically to protect mobile endpoints for SMBs. These are the characteristics that make Webroot Mobile Protection a logical choice for any SMB mobile security business plan:

- Integration with Webroot SecureAnywhere Business Endpoint Protection
- Cloud-based for increased agility and lower costs
Specific features for the mobile workforce, including advanced antivirus, Internet security and identity protection security that provides an application inspector, remote data wiping, lost device mapping, a virus shield, SIM card locking, network connection monitoring, device lock, device scream and much more.

Simple manageability of mobile devices and PCs from a single point of control.

Bulletproof protection, including the use of the Webroot Intelligence Network, which delivers constant threat updates.

Highest levels of performance, including a simple-to-install light client that won’t impact the user experience.

Over-the-air deployment for elastic scalability and simple rollout to devices via e-mail, SMS or QR code.

Support for multiple mobile operating systems, regardless of form factor.

Conclusion

The shift to a more mobile workforce and business environment is taking place, dramatically, right before our eyes. We are seeing the rise of mobile applications and the use of smaller consumer devices for all types of applications. And we are seeing those same devices being used for business applications as well, sometimes with the support and approval of the business, but more often without proper safeguards in place.

For SMBs, the opportunity to get mobility under control is at hand, which means addressing the ongoing, evolving and increasingly dangerous threat landscape. The advent of cloud-based services for security makes it much simpler for SMBs to take control: They can deploy a state-of-the-art solution immediately, without a significant up-front investment in infrastructure.

Webroot Mobile Protection is one of the first cloud-based solutions that specifically addresses the challenges SMBs face in supporting mobile devices and mobile workers. It provides a full suite of mobile protection features, while delivering cost efficiencies, simple manageability and high performance. The threats are out there now, and they are increasingly
targeting both SMBs and mobile workers. Isn’t it time to make sure your organization is adequately protected?

For a free 30-day trial of Webroot Mobile Protection, go to http://www.webroot.com/techmobiletrial