White Paper

New Services Driving Mobile Solutions

Exploring opportunities in BYOD and mobile device management

A solution provider's role is all about serving as a trusted advisor to his or her client. Often that means helping them with their clearly identified business problems. But it also requires noting gaps that the clients themselves may not have noticed. Such is the case with mobile devices.

The global smartphone audience surpassed 1.75 billon in 2014, according to eMarketer, and in a growing number of countries, more than half of mobile phone users use smartphones[i]. People tend to carry their smartphones everywhere. They not only bring them to work, they also use them for work, no matter the size of their employer.

Companies call it BYOD (Bring Your Own Device). The challenge of managing BYOD has been a hot topic in enterprise circles, but less so among SMBs (small and mid-size businesses). But the truth is that the issue of employee devices is both a hurdle and an opportunity for all businesses, no matter the scale.

In fact, SMB employees are less likely than enterprises to have sufficient infrastructure to support BYOD device usage or security to protect the sensitive company data they contain. A survey by IT community site Spiceworks found more than 60% of small businesses are currently supporting personal devices employees bring to work, with 23% calling BYOD a real headache for IT support[ii].

SMB's pains are solution providers' opportunities. So is there a market for solution providers in reselling services around BYOD, such as mobile device management?

The State Of Mobile

Because of the mobile trend, SMB business software is enabling remote access via mobile devices to increase user productivity and customer service. Remote access enables mobile workers to add value and transact business in real time, no matter where they are: They can issue instant price quotes, monitor dashboards, check inventories, access schematics, schedule services, and even collect payment.

"One area that is vital to an SMB's efficiency is mobility," says SMB research firm AMI Partners[iii]. "The ability to work on the go has resulted in a boost in overall productivity and competitiveness for many companies."

But the flip side to all that access is risk. SMB employees are essentially walking around with the well-marked keys to the business' front door—keys easily left behind on a restaurant table, swiped from a pocket or exploited by a disgruntled former employee. In the wrong hands, the phone provides easy access to customer, product, financial and other sensitive data. A breach not only harms the SMB's reputation, but exposes them to lawsuits and prosecution.

A misplaced device is not the only risk posed by employees' devices: Data thieves are also gaining remote access to devices and networks. Mobile operating systems are increasingly vulnerable to malware, with Android a particularly popular target. According to a report from Alcatel-Lucent, mobile malware infections increased 20% in 2013[iv]. Android devices accounted for 60% percent of total mobile network infections.

So the same mobile devices that are enabling business are driving up SMB risk. As SMB's trusted ad- visors on IT and data, solution providers are well positioned to help their clients understand all aspects of what mobile means to their businesses: opportunities for increased productivity and customer service, but also the inherent vulnerabilities. Solution providers can offer risk assessments to their SMB clients to establish the current state of network security as well as the array of BYOD devices in use.

SMBS Need BYOD Policies

One important step in counseling SMBs on containing BYOB risk is to help them craft clear policies for their employees' mobile devices. According to VDC Research, just over 40% of organizations of all sizes currently have a BYOD policy, and another 34% plan to create one[v].

"Development and implementation of effective BYOD management initiatives are immense challenges for any organization," says VDC's report. The need for security must be balanced with employee demands for mobile technical support, access to corporate systems and flexibility in choosing devices.

Gartner recommends that BYOD policies specify the following:

- which platforms will be supported and how
- what service levels a user should expect
- what the user's own responsibilities and risks are
- who qualifies
- guidelines for employees purchasing a personal device for use at work, such as minimum requirements for operating systems[vi].

Such BYOD policies help SMBs contain the costs of supporting their employees' devices. Right now the average corporate IT department supports 3.9 different mobile OSes, according to VDC[vii].

One of the stickiest BYOD topics is security. Be- cause the employee, not the SMB, owns the de- vice, it can be difficult to know what actions the SMB can take to protect its data. Should a breach occur, does the business have the right to wipe the device's memory? Unfortunately, the ability to segment business from personal data on mobile devices is in its infancy, so a remote wipe would eliminate employees' personal, as well as company, data.

Such challenges are driving some SMBs to consider paying for some or all of the mobile device as a way to create an implied right to govern device use and maintenance.

Some companies subsidize their employees' pur- chase of devices or provide a stipend. Others are purchasing mobile hardware and mobile broadband contracts for their employees, who can use these devices for business and add personal data if they choose. AMI forecasts spending on smartphone devices and data plans among SMBs worldwide to increase by 12% through 2018. Also, adoption of tablet devices and data plans is expected to increase twice as fast as smartphones[viii].

Lack of clear BYOD policies drives up cost and in- creases security risk for SMBs. Solution providers have an opportunity to assist SMB in developing BYOD policies based on experiences with similar businesses. Sound guidance from solution providers will help these businesses maximize the benefits of BYOD while minimizing the cost and risk.

A Role For Mobile Device Management

Mobile device management software is another important way to balance the opportunity and risk in BYOD. MDM enables IT professionals to provision, configure, monitor, track and secure mobile devices as users access business data and applications.

But SMBs have not adopted MDM solutions in large numbers. The Spiceworks study[ix] found that:

- 61% of SMBs have implemented a BYOD policy or initiative
- Of those SMBs, 17% are actively managing mobile devices using an MDM solution, with 20% more planning to address this in the next six months
- 56% currently have no plans to implement an MDM solution

According to the report, 49% of those not adopting MDM do not perceive big enough security threats to warrant the investment. More than a third (36%) say they lack the knowledge to proceed with implementation and 34% cite budgetary concerns.

Those are troubling figures for those seeking to re- sell MDM solutions to SMBs. Unfortunately, those businesses leave themselves open to considerable risk of intrusion, data theft, unauthorized use and malware infections.

It's important to educate clients about these risks, but it's clear that won't be enough to move many SMBs toward adopting MDM as a point solution. Instead, solution providers are advised to include MDM as part of the integrated services suites they use to support SMBs' complete IT environments.

The Mobile Opportunity

Mobility is changing the way business is conducted, helping workers in both SMBs and enterprises to become more productive and enhance service to customers. But along with data portability and remote access comes risk. As their trusted advisors, solution providers are well-positioned to help SMBs understand and ad- dress the vulnerabilities that mobility introduces:

- Offering education and risk assessments to establish the current state of network security as well as the array of BYOD devices in use.
- Assisting SMBs in developing BYOD policies based on their experiences with similar businesses.
- Building MDM into their services suites to manage and secure mobile devices as their users access business data and applications.

As the risks inherent in BYOD become increasingly clear, SMBs will expect to see mobile device management in the solution set of their trusted IT partner. Solution providers must consider the state of BYOD risk among their clientele and integrate MDM into their offerings.

About AVG Technologies (NYSE: AVG)

AVG is the online security company providing leading software and services to secure devices, data and people. AVG has over 187 million active users, as of March 31, 2014, using AVG's products and services including Internet security, performance optimization, and personal privacy and identity protection. By choosing AVG's products, users become part of a trusted global community that engages directly with AVG to provide feedback and offer mutual support to other customers.

Keep in touch with AVG


Blogs

Contact AVG

United States:
AVG Technologies USA, Inc.
2105 Northwest Blvd.
Newton, NC 28658,
U.S.A.

casales@avg.com
1-855-254-6987

United Kingdom & Ireland:
AVG Technologies UK Ltd
Olympic House,
995 Doddington Road
Lincoln, LN6 3SE
United Kingdom

sam@avg.com
+44(0)1522 803285

Canada:
AVG Technologies Canada Inc.
309 Legget Drive,
Ottawa, ON, K2K 3A3,

Canada.

casales@avg.com
1-855-254-698

Australia & New Zealand:
AVG Technologies AU Pty Ltd
47 A Wangara Rd
Cheltenham Victoria 3192
Australia

mmwp@avg.com.au
Australia: 1300 284 000
New Zealand: 0800 284 000

Rest of World:
AVG Technologies CZ, s.r.o.
Karla Engliše 3219/4
Praha, 150 00,
Czech Republic

reseller@avg.com
+420 549 524 011

Head Office:
AVG Technologies, N.V.
Gatwickstraat 9 -39
1043 GL Amsterdam
Netherlands

reseller@avg.com
+420 549 524 011