Laurie McCabe, Partner
Sanjeev Aggarwal, Partner

Finding Balance:
A New Security Approach for SMBs

Sponsored by: Dell

Top Takeaways

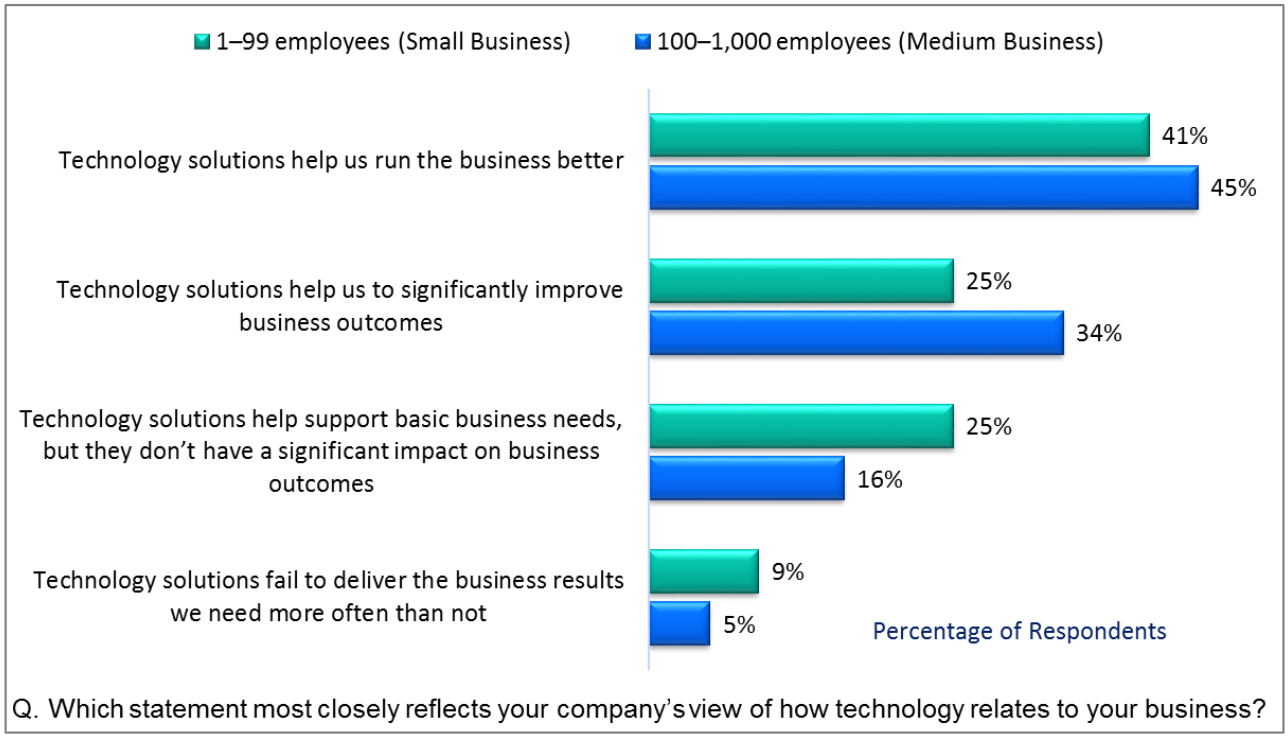
- As SMBs rely more on technology to run their businesses, the requirements to secure and protect data and access become more critical.
- SMBs rank security as a top technology challenge, but the magnitude of cyber-security issues and risks can be overwhelming due to limited IT staff and budgets.
- By taking an automated, policy-based security approach, SMBs can keep pace with new technologies while gaining assurance that critical corporate data is safe.
- A multilayered, rules-based approach to secure user devices, data and the corporate network makes it easier to enforce policies, protect assets and block malware.
- Look for a provider with a strong security portfolio, track record and market footprint that can tailor solutions to your business today and adapt to your requirements as they evolve.

The way people work has dramatically changed. The Internet, cloud computing and mobile solutions have empowered people with the freedom and flexibility to do their jobs more easily and quickly than ever before. At the same time, new technologies continue to expand the volume and variety of data at our fingertips, enabling people to create and share information in new ways.

Our ability to access information from anywhere, on any device and in real time is radically reshaping the way we collaborate, communicate, transact and make decisions. Today, 25% of small and 34% medium businesses (SMBs) view technology as helping them to significantly improve business outcomes, while 41% and 45%, respectively, agree that technology helps them to run their businesses better (Figure 1). Businesses are using technology not only to automate operations and gain efficiencies, but also to improve customer engagement, enter new markets and create entirely new, disruptive business models.

©SMB Group, Inc.

Figure 1: SMBs View Technology as Key to Success



Source: SMB Group 2015 SMB Routes to Market Study

The upside is proving to be enormous. Dell's Global Technology Adoption Index (GTAI 2015) finds that enterprises using new technologies including big data, cloud computing and mobile solutions have up to 53% higher revenue growth rates than enterprises that don't.

But as SMBs rely more on technology to run their businesses, the requirements to secure and protect data and access become more critical and complex. Even large companies can find the sheer scope of potential cyber threats overwhelming. SMB Group research shows that medium businesses rank security as their second-most-pressing technology challenge, and for small businesses, it's number one.

Although the challenge is daunting, SMBs need to address security in a practical, effective way. With a thoughtful, proactive approach, SMBs can strike the right balance and take advantage of the latest mobile, cloud and analytics technologies while also protecting the data that these technologies allow us to access so freely.

SECTION 1: TECHNOLOGY TRANSFORMS THE WAY WE WORK

People are racing into the digital, mobile and social future at breakneck speed. Technology is transforming employee interactions, changing how data flows within an organization, as well as between the organization and its customers, partners and suppliers. The "cloud first, mobile first" millennial generation is accelerating these trends and raising expectations for anytime, anywhere access and social, analytic and collaborative capabilities.

Cloud and mobile solutions are already playing a big role in SMBs. Benefits such as cost effectiveness, flexibility, and easier and faster deployment are driving SMB adoption of cloud applications and storage solutions (Figure 2). The cloud gives SMBs the opportunity to harness more of the solutions that they need to get ahead—solutions that many would never have been able to deploy and manage on their own before.

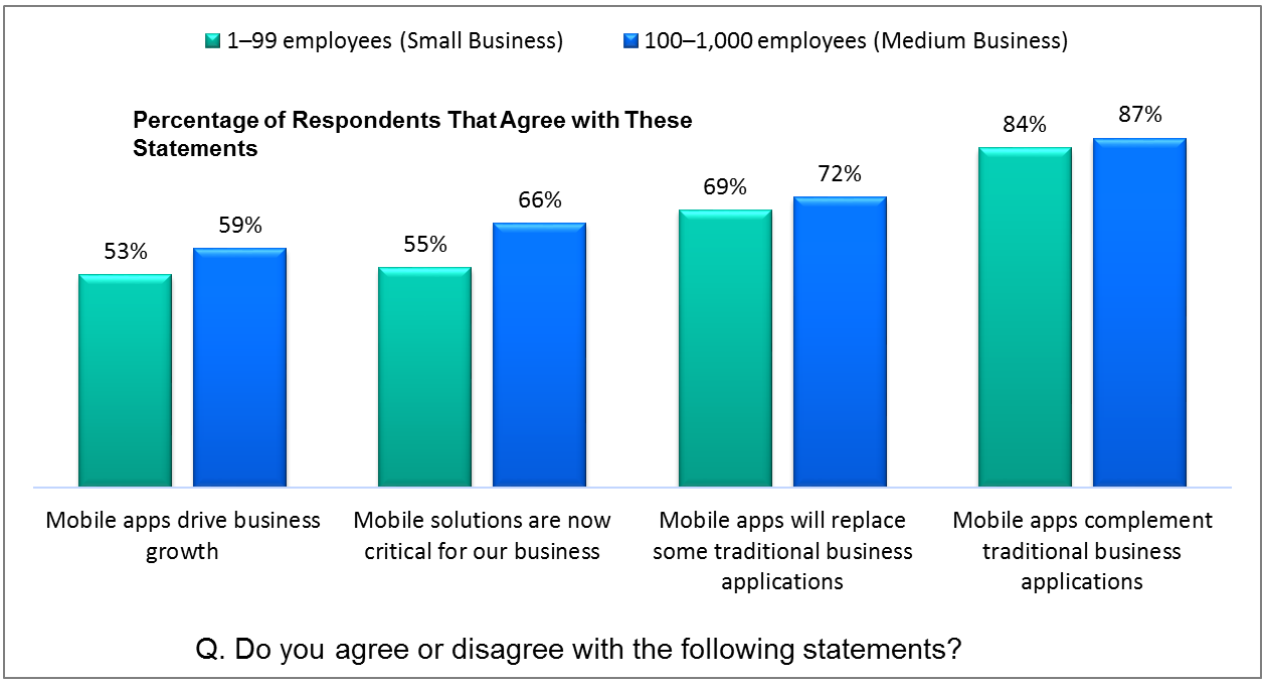
Figure 2: SMB Cloud Drivers and Adoption

Source: SMB Group 2015 SMB Routes to Market Study

Meanwhile, SMB adoption of mobile solutions has been nothing short of revolutionary. SMB Group research shows that the overwhelming majority of SMBs already use mobile collaboration apps, such as mail, calendar and contacts, and many are now using mobile business apps, such as payment processing, expense management and time management. As indicated in Figure 3, a solid majority of SMBs agree or strongly agree with the following statements:

- Mobile solutions are now critical for their business.
- Mobile apps are complementary to current business applications.
- Mobile apps will replace some of their existing business applications.
- Mobile apps drive business growth.

Figure 3: SMBs View Mobile Solutions as Critical to the Business



Source: SMB Group 2015 SMB Routes to Market Study

All indicators show that SMBs will continue to expand mobile solutions to more employees and for more uses. According to SMB Group's 2014 SMB Mobile Solutions Study, 64% of SMBs plan to increase spending for mobile applications, services, management and devices.

"Bring your own device" (BYOD) is a big part of the mobile phenomenon. SMB Group research indicates SMB BYOD adoption is growing, with 59% of SMBs now supporting BYOD so that their employees can work the way they want on the devices with which they're most comfortable.

The convergence of new digital technologies also means that we're creating more data with each passing day. According to International Data Corp. (IDC), by 2020, 450 billion Internet transactions will be conducted each day, generating 240 exabytes of content. Of course, companies want to mine this data for better insights into their business, customers and partners. New analytics solutions are

making it increasingly easy to store this data in the cloud and access it from a smartphone or tablet, empowering businesses with insights to make better decisions. So it's not surprising that SMB Group's 2015 SMB Routes to Market Study shows that 30% of small and 46% of medium businesses rate analytics solutions as one of the top three most critical areas for investment.

The writing is on the wall: SMBs need to proactively deploy technology to improve business processes, to keep pace with customer expectations and to differentiate and innovate. SMBs that use technology to stay ahead of their customers' demands will thrive, while those that don't will face extinction.

SECTION 2: THE GROWING SECURITY CHALLENGE

The growth of data, mobile devices and solutions, cloud computing and other disruptive technologies have yielded an unintended result: data is no longer tied to a specific device. Because data can now "live" in more places, the risk of data loss and leakage—whether from accidental or malicious causes—increases. In other words, as we put more information into the right hands, we also increase the likelihood of putting it into the wrong ones.

The sheer magnitude of cyber-security issues and risks—such as honeypots, worms, hijackings, trojans, trampolines, phishing and ransomware—is enough to make anyone's head spin. Cyber criminals have increasingly more avenues to access invaluable company information both in traditional ways, such as device theft, and by using newer methods such as drive-by downloads, which happen when malware is automatically downloaded to your computer from a website without your consent or even your knowledge.

And while malicious, external risks from cyber criminals capture most of the headlines, internal threats from employees, contractors or associates—who may either intentionally or accidentally jeopardize security—can be just as debilitating. Accidental breaches can occur, for instance, when employees connect personal Internet accounts to company devices or use weak passwords. On the malicious side, company data can be compromised when people misuse legitimate privileged access to corporate data and systems.

SMB Group research shows SMBs rank security as a top technology challenge—and for good reason:

- According to a February 2014 survey commissioned by Dell and researched by Vanson Bourne, approximately three-quarters of IT decision makers experienced a security breach in the previous year.
- In its Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015, PricewaterhouseCoopers (PwC) reports that midsize companies (revenues between $100 million and $1 billion) are increasingly coming under attack, possibly because they don't have the same levels of security as large companies.

End users of all types are easy targets for cyber criminals. One stolen (or even lost) laptop or smartphone with access to company data can provide a criminal with access to sensitive information that can result in brand damage and financial losses.

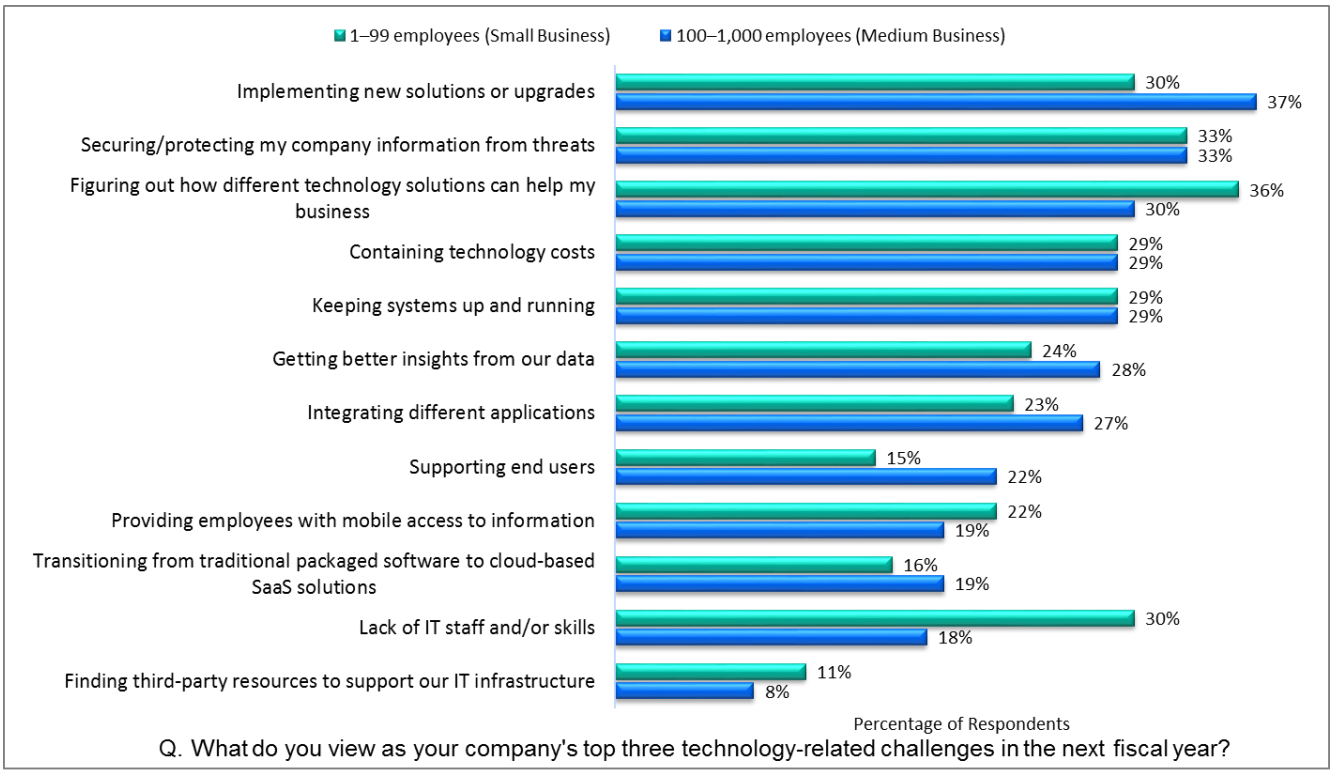
Today's networks are also more complex than ever before. The formerly clear demarcation between the network and the Internet has blurred. Employees, customers and partners are all likely to need remote access. Employees are using Android-, Apple- and Windows-based smartphones and tablets to connect to email and other apps and data. According to SMB Group's 2014 Small & Medium Business Mobile Solutions Study, 58% of small and 61% of medium businesses view concerns about data, network or transaction security as the top obstacles to expanding their use of mobile devices and solutions.

Employees and external stakeholders are storing and accessing data in the cloud as well. It's easy for end users to create accounts and store data on Dropbox or Google Drive. As the volume of data and the number of places we can store that data increases, many SMB IT organizations don't even know where all of their data resides.

Amid all of this, SMBs must figure out how to protect their data with limited IT staff and budgets—there are no chief security officers in SMBs! SMB Group research indicates that on average, only 22% of businesses with fewer than 100 employees have full-time, dedicated IT staff, and 31% have no IT support at all. Meanwhile, although 85% of medium businesses have dedicated IT staff, these employees are likely to be IT generalists.

SMBs face a difficult dilemma. As technology becomes an increasingly important part of the business fabric, the challenges to manage it grow (Figure 4). SMBs struggle to deploy new solutions—and have trouble figuring out what solutions will work best for them in the first place. This leaves most SMBs unprepared to deal with today's threats—let alone those that big data, the Internet of Things (IoT) and other emerging technologies will usher in tomorrow.

Figure 4: Top Technology Challenges for SMBs



Source: SMB Group 2015 SMB Routes to Market Study

Yet all too often, SMBs choose not to see themselves as potential cyber targets. But as larger enterprises implement more sophisticated data security solutions, cyber criminals may be inclined to target smaller businesses that might have weaker security measures in place. And because SMBs are often digitally connected to larger business partners, they are increasingly attractive targets. Hackers can potentially gain access to not only SMBs' data, but also data of their bigger partners.

According to Endurance International Group's 2015 Small Business & CyberSecurity Survey, 31% of small businesses have experienced a cyber attack or an attempted cyber attack. However, despite these concerns, fewer than half (42%) of survey respondents have invested resources in cyber-security protection in the past year.

User devices provide cyber criminals with an enticing point of entry into a business's network. SMBs need to ensure these devices aren't being abused—but if security measures are burdensome, end users will try to bypass them if it's easier to do so. In fact, ITIC survey data shows 35% of firms don't know if or when BYOD mobile devices have been hacked! Obviously, if you don't know you have a problem, you can't fix it.

SECTION 3: INTELLIGENT DATA SECURITY SOLUTIONS: A BETTER WAY TO THINK ABOUT SECURITY

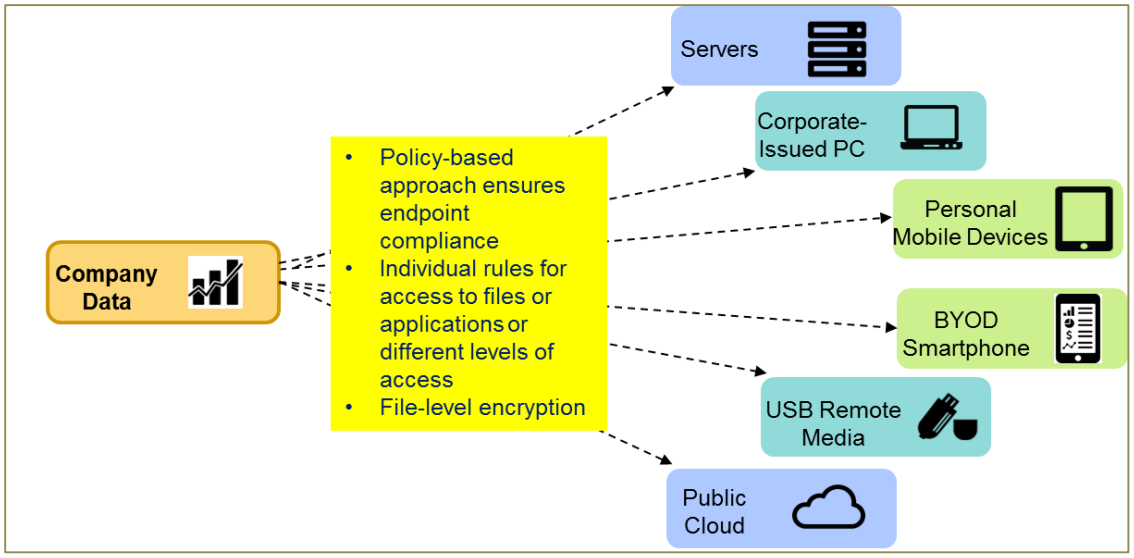
It's not a lack of security solutions that keeps SMBs from taking action, as there are hundreds of them on the market. But most security vendors have taken an approach that is hard for SMBs to warm up to: using the FUD (fear, uncertainty and doubt) approach to ratchet up anxiety about potential threats to scare SMBs into buying their solutions. Consequently, SMBs too often end up feeling overwhelmed, confused and totally inadequate to deal with the magnitude of the situation. But there's a high cost to pay when you bury your head in the sand or rely on security solutions that may have been adequate a few years ago but are no longer sufficient.

So how can SMBs procure new technologies that help move the business forward while simultaneously protecting against evolving security threats to user devices and corporate networks and data? The questions of what to secure as well as when and how to secure it are complex. But every organization has valuable or sensitive data and must protect that data because security breaches have grave consequences, especially if cyber criminals steal data.

SMBs need a better approach—one that makes security a manageable challenge instead of a bewildering, unsolvable nightmare. They need a plan that enables them to continue taking advantage of the latest mobile, cloud and other technology advancements and offers them peace of mind that their biggest risks are being managed.

Endpoint security management provides a policy-based approach that requires endpoint devices to comply with specific criteria before they are granted access to network resources (Figure 5). Endpoints can include any user device, from PCs and laptops to smartphones and tablets, as well as specialized devices such as point-of-sale (POS) terminals and bar code readers.

Figure 5: Endpoint Security Management



Source: SMB Group

Endpoint security solutions are deployed on both the client side and the server side, enabling centralized monitoring and management on the server. These solutions can be run in-house or in a cloud model, where a software vendor or managed service provider (MSP) manages the solution remotely. In either case, endpoint security management solutions determine the status of a user's device when it connects to the network, checking to ensure that the operating system, the browser and other applications are in compliance, and whether antivirus, firewall and other security components are updated. If a device is non-compliant, it can be either updated from the server or denied access to the network.

Policies can be created to set individual rules for access to files or applications or different levels of access (such as read-only, update or delete permissions for files). They can be established to allow users to access files only from certain locations or geographies and not others, to enable or disable users' ability to print or transfer files to USB sticks or to other systems, and to automatically encrypt files. This type of approach enables organizations to protect corporate data regardless of where it resides.

SECTION 4: GETTING STARTED WITH ENDPOINT SECURITY MANAGEMENT

There are many endpoint security solutions available. To begin the process of selecting and purchasing a solution, SMBs should conduct a realistic internal risk assessment to determine what potential vulnerabilities pose the biggest financial and brand threats to the business (Figure 6).

Figure 6: Start with a Realistic Internal Assessment

Source: SMB Group

Both business stakeholders and IT must help move the focus of purchase discussions away from technology considerations and toward critical business vulnerabilities, with business decision makers helping to identify, quantify and prioritize them. What would happen if certain sets of data were breached versus other sets? For example, it probably is more important to first protect patient records in physicians' offices rather than expense account data. Some data must also be secured to meet specific regulations set by government agencies, such as HIPAA regulations for healthcare providers.

This type of internal audit will help SMBs distinguish between the data they care most about and the data that is less important to protect, so businesses can apply the bulk of their budget and resources to protect the "crown jewels" with more stringent controls. An audit should also shed light on security vulnerabilities that have a high potential for breaches but are relatively easy to fix by providing an alternative action. For instance, if employees use USB sticks to transport data, IT could create a secure portal to transport data instead. Identifying security gaps helps to calculate risk and arms SMBs with the knowledge required to build a security plan that factors risk and resources into the equation.

For most end users, convenience trumps security. Therefore, as SMBs consider key vulnerabilities, they also must involve end users to understand their needs and meet them in a more secure—yet still relatively painless—way.

SMBs should avail themselves of trusted advisors—whether security vendors or their partners—to help think through these issues. It's important to have a good grasp of what vulnerabilities are most likely to trigger disruptions and what the impact would be on the business, as well as to develop a risk management plan that aligns with the business's requirements in this area.

This type of assessment enables companies to establish or revise baseline risk management policies and procedures. In Vanson Bourne's survey of IT decision makers, more than half (55%) of respondents reported that setting policies for information management is a priority. Specifics SMBs might address are which data sets are the most important or must adhere to regulations, which employees have had access to what information, password requirements, use of removable media, mobile device and wireless usage, and data protection, backup and destruction. SMBs should make sure their policies are easy to understand and apply, and it's important to remember that the policies will need to be revisited regularly as the company develops a more comprehensive approach and as business requirements and the threat landscape evolve.

With a shared understanding of critical vulnerabilities and key priorities as a starting point, SMBs can avoid the pitfalls of under protecting highly sensitive data and overprotecting—and probably overspending on securing—less critical information.

SECTION 5: KEY CONSIDERATIONS FOR A SECURITY APPROACH THAT KEEPS PACE WITH OPPORTUNITY

In general, endpoint security solutions work as follows: you input business policies and rules into the solution, and then it communicates to the network how to support those policies. The solution should help you manage all of your endpoints—whether they're running Windows, Apple, Linux or Android operating systems. Other considerations include the following:

- **What malware security features are included?** These features can span from basic malware detection capabilities to advanced malware prevention. Helping administrators secure the entire network—through such services as network access control, email security, gateway protection and remote workstation security—is important as well.

- **How well does the solution protect against malware? How does it stack up in independent tests across different operating systems and devices?** Finding the answers to these questions will help you understand how well the products will work in your business.

- **What other security measures does it enable you to activate?** Endpoint security solutions go well beyond malware protection. They also can include solutions that enable you to set up other protections, such as safeguarding against data loss by locking down network access, controlling the types of data end users can transfer and configuring policies for employee-owned devices. For instance, some solutions can prevent users from sharing specified files via email, instant chat or Internet uploads, or they can encrypt data that is sent to the cloud. Other key measures include encryption to protect data regardless of where it resides (laptops, smartphones, USB keys, etc.); identity and authorization capabilities to verify who is accessing the data, such as biometrics; and two-factor authentication, which requires not only a password and a username, but also something that only the user has access to.

- **How easy is the system to administer and manage?** Look for capabilities that make things easier for IT, such as a modern user interface, and centralized management consoles to help deploy software, control remote devices and manage user profiles. You'll also want tools that make it easy to create reports, transmit and manage updates and patches, detect new endpoints, and audit software and hardware. Some solutions even provide templates for government compliance reports. In today's mobile age, solutions should also offer remote management capacities so IT can spot and fix issues from their mobile devices.

- **Does the solution enable you to take an incremental, multilayered approach?** As discussed earlier in this report, SMBs typically suffer from a dearth of IT resources and don't have the time or money to do everything all at once. Endpoint security solutions that address this problem allow you to address the most sensitive data requirements and controls first and then add on new protections in an integrated manner later. Because a multilayered approach offers integrated modules that you can add as needed, they are typically easier to tailor to the security, privacy and compliance needs of each individual SMB. For example, physician offices will have different priorities than a manufacturer or a

bank. SMBs can have assurance that each piece of the puzzle will fit together regardless of whether they implemented everything all at once or gradually over time, and that the solution can scale to fit a company's needs, timetable and budget. Because they work in tandem, modules can be centrally managed as well, giving IT staff a holistic view of all deployed components.

- **Does the solution and/or provider help to facilitate moving data off end-user devices?** As mobile device use soars, data "lives" on an increasing number of devices. However, it's not the stolen laptop or hardware that represents the greatest threat or loss; it is the data that both resides on that device and is accessible from it. Work with providers that can help you move more of your critical data off of endpoint devices and into a secure private or public cloud.

- **Is the solution built with a realistic view of end-user psychology?** People need to get their jobs done. Solutions that put too many barriers between an employee and necessary data increase the chance that employees will get frustrated and create a workaround that can cause a data breach. Of course, the solution should protect data on multiple devices and platforms, including BYOD. Ideally, the security would be seamless or "invisible" to end users, allowing them to work the way they want, when they want.

- **What kinds of service and support does the provider offer?** Narrow down your short list to experienced, proven providers with a strong track record of helping businesses with requirements similar to your own. Taking time to understand your specific needs and providing best practice advice to help you achieve the best outcomes are also critical criteria. Because SMBs often have smaller IT staff than larger companies, the data security vendor must be able to partner with the SMB to successfully implement the solution. SMBs should look for providers that complement their internal IT staff. An effective vendor will understand the complexities of a company's business, design a solution that tackles these security complexities and help a company to scale as needed. On a more tactical note, look for capabilities such as 24/7/365 support, on-site assistance and training as needed, access to a dedicated account manager, and access to user communities to help you think through and address use issues as needed.

SUMMARY AND PERSPECTIVE

As SMBs rely more on technology to run their businesses, the requirements to secure and protect data and user access will continue to multiply. Just one serious targeted attack can potentially put an SMB out of business, while a severe privacy violation—such as the loss or theft of patient or client financial data—can cost a company millions in terms of brand damage and lost business.

But although you can't eliminate every risk, you can address the biggest vulnerabilities for your business by taking a thoughtful, proactive approach to security that enables you to keep pace with new technologies while gaining assurance that your critical corporate data is safe.

Endpoint security management offers SMBs a holistic, rules-based approach to make it easier to enforce policies, protect assets and block malware. By automating many security functions, SMBs can also reduce the human resources needed to protect the organization.

Using a multilayered approach, endpoint security solutions allow you to address the most sensitive data requirements and controls first, and then add on new protections in an integrated manner later. Consequently, they can also be easily tailored to the security, privacy, compliance and budgetary needs of each individual SMB. As important, different modules work together and afford the advantages of having a holistic view of all deployed components and centralized management capacities.

SMBs have many choices when it comes to endpoint security solutions. To select the best fit for your business, start by mapping solution functionality to your specific requirements. Select a proven provider with a strong track record that also takes the time to understand your specific needs and can provide consulting, deployment and support services to help you meet both business and security goals. Finally, because the security landscape is constantly in flux, look for a provider with a strong security portfolio and market footprint that can tailor solutions to your business today and adapt to your requirements as they evolve.

SMB GROUP, INC.

SMB Group focuses exclusively on researching and analyzing the highly fragmented "SMB market"—which is composed of many smaller, more discrete markets. Within the SMB market, SMB Group's areas of focus include Emerging Technologies, Cloud Computing, Managed Services, Business and Marketing Applications, Collaboration and Social Media Solutions, IT Infrastructure Management and Services, and Green IT. Read our 2016 Top Ten SMB Technology Trends for our views on game-changers in these and other areas of the SMB market.