Building a Business Case:

Cloud-Based Security for Small and Medium-Size Businesses

table of contents

A TechTarget White Paper brought to you by Symantec

TechTarget Custom Media

Investing in IT security is one of the most important strategic decisions for executives at small or medium-size businesses. The damage caused by a security breach could have dramatic consequences: A single security breach can cost a company millions of dollars, and malicious attacks are the most costly of all data breaches.[1]

And don't think because your business is small or medium-size it isn't vulnerable to attack. In fact, your size may make you even more vulnerable: Since the beginning of 2010, 40% of cyberattacks have been targeted at SMBs, versus 28% against large enterprises.[2] And in 2012, attacks against SMBs doubled compared with 2011,[3] with the average business facing 5,000 sophisticated malware threats alone every month[4] and the number of malicious new URLs growing by 30,000 every single day.[5] Some cybercriminals are even using SMBs as a way to find a backdoor into larger organizations, which means a lack of adequate protection may not only make your business more vulnerable, but it could also severely impact your partner relationships.

The unfortunate reality is that far too many SMB executives are unaware of the types of threats they face and are not doing nearly enough to protect their organizations against potentially crippling attacks. Nearly 90% of SMBs have no formal written Internet policy for employees, 70% do not have policies for social media use, and 69% don't even have an informal Internet security policy to provide users with commonly accepted guidelines on how to use the Internet.[6] With no policies in place at all, users are pretty much free to do whatever they want, including visiting non-business or nefarious websites, such as those devoted to gaming or pornography, that might leave the company more vulnerable to attack.

Clearly, with the number of threats escalating, the sophistication of the threats increasing, and the growing vulnerability of SMBs as a target, something has to be done to alter the course for small or midsize organizations. To avoid major consequences, they must shift their mindset and approach from one of being merely reactive to a position where they are installing effective and proactive defenses.

1 2011 Cost of a Data Breach Study: United States, Ponemon Institute, March 2012
2 SMB Threat Awareness Poll, Symantec, November 2011
3 New Survey Shows U.S. Small Business Owners Not Concerned about Cybersecurity; Majority Have No Policies or Contingency Plans,
4 National Cyber Security Alliance and Symantec, Oct. 15, 2012
5 Blue Coat Systems 2012 Web Security Report
6 Security Threat Report 2012, Sophos

Key Business Drivers

For SMB executives, building a business case for investing in endpoint security comes down to answering a few fundamental questions. How much will it cost? More important, how much will it cost to get the right amount of protection? What are the risks of making this investment – or, with security, what are the risks of not making the investment? Where is the organization most vulnerable, and how does the organization ensure it is delivering adequate protection where it is most likely to face attacks? How can the company ensure protection for the future, even as cybercriminals change their tactics and seek to exploit new weaknesses?

In many ways, investing in security is akin to buying an insurance policy: You hope you never need it, but when you do, you thank your lucky stars you had it in place. It could, in fact, save your business.

A few things will become clear as you start delving into these questions:

1. Focus on Risk Management: Not investing in adequate security is not really an option. The consequences of a successful attack are too great, and the potential solutions to achieve solid protection are relatively inexpensive. In fact, as you'll see below, by using a cloud-based service for security, you will be able to minimize your investment and manage endpoint security so you are only paying for the security you need. Any cost analysis looking at risk vs. reward will tell you that investing in IT security is one of the smartest business decisions you can make.

2. Protect Your Endpoints: This is where your business is most vulnerable to attacks. Cybercriminals always focus on your weakest links, and because many SMBs don't protect them well enough, endpoints are where the threat of attack is often the greatest. Criminals are increasingly exploiting everyday activities that make users more vulnerable, such as using email, search engines, social media and popular websites. As many as 30,000 malicious websites are being created every single day.[7] Without proper security safeguards, every user on any device on your network has the potential to bring harm to your organization, by inadvertently downloading a virus or piece of malware or perhaps through malice or negligence, such as losing a laptop.

[7] Security Threat Report 2012, Sophos

3. Explore the Cloud: The availability of robust cloud-based security-as-a-service solutions is one of the most important innovations taking place in IT security today. The benefits of cloud-based security for SMBs can be dramatic, including lower costs with predictable pricing, state-of-the-art protection that is constantly updated to address the evolving threat landscape, and simple deployment, upgrades and provisioning. In addition, a cloud-based solution enables simple scalability as you add new users to your organization.

Each business is different and, as you dig deeper into building your business case for a successful security solution, there will likely be many key factors to consider. How big is your IT staff, and how well versed are they in managing security threats? How much time and effort do you want to spend on managing security and deploying security solutions, such as patches and updates? How mobile is your workforce, and how much more mobile will it be over the next few years? Do you support remote workers and/or do you plan to support them in the future? How can you ensure that the security solution you deploy does not have a negative impact on application performance or on the productivity of your workers?

The Business Case for Endpoint Security in the Cloud

If you examine all of your business drivers for endpoint security, you will discover that deploying a cloud-based service from a leading vendor such as Symantec will help you achieve all of your key objectives, including reducing costs and risks as well as providing the highest level of protection for your endpoints and your business. Here's how:

- ROI and cost containment: Building your own on-premises security solution can be extremely expensive. You have the up-front costs for hardware and software, and then you have ongoing costs for maintenance, support and upgrades. A cloud-based service eliminates the need for any initial investment and enables you to take advantage of a subscription model that tends to be both inexpensive and predictable. You pay only for the services you need, for the specific devices that need protection. As you scale up with new users, you can simply add them without purchasing new servers.

- Bulletproof protection: One of the biggest advantages of a cloud-based service is that you are putting your protection in the hands of security experts who can react quickly to new threats. Cloud services can stay one step ahead of premises-based solutions because they can deploy the latest security advances immediately, as they become available. With the right cloud-based solution, such as Symantec™ Endpoint Protection Small Business Edition 2013, your business is protected with the most advanced antivirus and anti-malware technologies, keeping your servers, desktops and laptops safe from viruses, worms, Trojans, spyware, bots, zero-day threats, rootkits and other types of attacks.

- Risk management: In addition to providing state-of-the art protection, a cloud-based solution can help you manage risks in other ways. For example, Symantec Endpoint Protection Small Business Edition 2013 enables always-on protection, so that updates take place transparently over an Internet connection as soon as they are available. This helps keep employee systems current and consistent with policies wherever they are, even if they are not logged into a virtual private network. This is an important feature for your mobile and remote workers, particularly if they are using less secure connections such as Wi-Fi to connect with the business. Also, the cloud-based delivery of Symantec Endpoint Protection Small Business Edition 2013 provides a service-level agreement that guarantees 100% Web console availability. This means you can rest assured that your business will always be able to make changes, as well as manage and deploy the service wherever needed. In addition, for an added level of protection, the Symantec cloud-based deployment allows SMBs to detect and protect against harmful files from USB storage devices.

- Simplified deployment and manageability: Cloud-based endpoint security is remarkably simple to deploy and maintain, and has a minimal impact on your IT organization. Compared with premises-based solutions, you can save money on IT resources and deploy IT personnel on initiatives that can help to grow your business. Symantec's Endpoint Protection Small Business Edition 2013 can be installed in minutes, with no special IT staff or training required. It is managed from a single console and deployed to endpoints via a

direct download, email invitations or a redistributable package. Once the agent is installed, preconfigured policies are enabled for antivirus, antispyware, firewall and host intrusion prevention. From the administration console, an administrator can transparently send out patches, updates and policy changes to all endpoints over the Internet. The console can also be used for ongoing maintenance, provisioning new endpoints, managing remote clients, viewing the status of endpoints and a wide range of other functions.

Conclusion

SMBs can no longer be complacent in the face of a security threat environment that is increasingly becoming more sophisticated and coordinated. Attackers have taken note of the weaknesses of many SMBs and are actively exploiting them as a gateway to their larger business partners. A successful attack can be devastating, and without the right protection in place, it can seem to come out of nowhere. In today's environment, with the availability of robust endpoint security solutions offered as a cloud-based service, deploying state-of-the-art security can be done inexpensively and quickly, without significant impact on your IT staff or your business operations. It's important to note, however, that not all cloud-based security solutions are created equal. You want to make sure that when you build your business case, you consider the reputation and credibility of your cloud partner and its ability to deliver the most advanced endpoint solutions to your organization – now and in the future. Learn how Symantec Endpoint Protection Small Business Edition 2013 can be your path to a safe and effective security solution in the cloud.