WHITEPAPER: MEETING THE CHALLENGES OF ENDPOINT SECURITY

Meeting The Challenges of Endpoint Security

Growing businesses face real difficulties in protecting their users, especially remote workers, while keeping management costs down.

Symantec.cloud™

Meeting The Challenges of Endpoint Security

Contents

Introduction

Delivering endpoint security in an increasingly mobile environment comes with some major challenges. Growing businesses know they need to protect their end-users from viruses, spyware and unauthorised intrusion. In fact, the majority use some kind of anti-virus software and firewall on their desktop and notebook PCs. But is it good enough?

According to research by PricewaterhouseCoopers[1], the vast majority of small and medium-size businesses (83 percent) suffered a security incident in the last year. Nearly half of them (43 percent) were virus infections. So, clearly there is a difference between what companies say they do about security and the results they actually achieve.

Complacency and risk

How do we explain this gap between needs and results? It comes down to several factors:

- **IT management bandwidth.** Without large It departments, it is hard for companies to check continuously that every PC has the latest patches, the correct anti-virus software and a fully up-to-date firewall.
- **More flexible and mobile working.** Flexible and mobile working has changed the nature of security. More than 63 percent of SmBs give their staff remote access to company systems[2]. If security software doesn't allow for remote management and remote updating, these users are at greater risk of infection.
- **Lack of integration.** Only large companies with large IT departments have a fully-integrated, coherent, multi-layered defence against security threats backed up by in-house security expertise. When you multiply best-of-breed point solutions for security what you get, in fact, is a mongrel.
- **Fast moving security threats.** The traditional model of a perimeter-based firewall and client-resident endpoint security provides a degree of security but also the risk of complacency. After all, the attacks continue, online criminals get smarter and new patterns of work create new risks. For example, targeted trojans and zero-day attacks are on the rise.

In short, businesses have got the message that they need anti-virus software and firewall protection on all their PCs (or 'endpoints') but they don't always have the right technology to do it well. The result is a false consciousness. They think they are safe, but they're not.

Business challenges

In addition, companies have challenges that make good security tough:

- **Lack of IT resources.** Most smaller companies rely on a handful of individuals, some with other responsibilities, and often a third party It consultant to manage their infrastructure. Without the resources and scale or a large IT department, it can be a struggle just dealing with routine user problems, let alone proactively defending the company against security threats.
- **No in-house expertise.** It is unlikely that a growing company would have a specialist IT security expert on staff. Most IT support firms do not have this expertise either. Instead, companies have to rely on the credentials and track record of software vendors.

[1] http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html
[2] Ibid.

- **Ad-hoc PC management.** Growing companies often have limited or non-existent PC management systems. This makes it harder to ensure that software installations are PC configurations are consistent and it also makes it harder to solve problems when they occur, especially for remote users.

- **Focus on more important tasks.** Quite rightly, companies tend to focus on growing the business rather than growing their It overhead.

Clearly, growing businesses need to take a new approach to ensure they stay protected, to look after remote users and to do all these things while keeping costs down and reducing the admin overhead.

The threats keep coming

Client-side vulnerabilities are the weakest link in the security chain, according to a SANS Institute report on the top ten cyber-security risks.[3] Online criminals exploit them using targeted email and 'drive-by' web-hosted malware. Up-to-date security software is the main defence but updating many PCs can be time-consuming, especially if PCs are not connected to the company network for a while. This delay can leave endpoints vulnerable for hours, or even days, before the patch is applied.

Delays increase risk, especially with zero-day attacks that strike hard and fast before security vendors can issue an update. The SANS Institute reports a rising number of these zero-day attacks over the past three years. A large IT department can throw resources at a problem like this, but a small to midsize company with, say 100 employees and one full-time IT manager, will always find it harder to react quickly.

Protecting mobile users

Mobile and flexible working is on the rise. It helps growing business attract and retain great talent and reduce the cost of office space. Also, more entrepreneurial companies like to spend more time with clients than they do in the office. So everyone's a laptop warrior now but what does this mean for security?

According to Gartner, companies that do not address mobile security risks properly will experience more security breaches and this will increase the costs per remote worker costs by a factor of ten.[4] In other words, security problems could erase the very benefits you hope to achieve by letting your staff out of the office.

There is little chance of that trend reversing. In the UK, more companies provide telework alternatives[5]. Around a third of UK companies have remote working schemes and one in eight employees of small and medium-size companies work remotely at least once a week. More than half of all companies give staff remote access to corporate systems.

In any company, managers love the idea of remote access and the productivity it brings, with one exception. The IT security manager is often the lone holdout who resists the practice, arguing that with company computers leaving the physical confines of the office, it becomes more difficult to retain control over it, how up to date the security software is, and what web sites the end user is connecting to on the Internet. When computers are safely inside the worker's cubicle, the IT manager can impose URL filters to keep out potentially dangerous web sites, prevent installation of unauthorised software, and regularly update security software. But what happens when those computers leave the office, or worse, when employees start using their unprotected, unfirewalled home computers and laptops to connect to the corporate intranet? It's anybody's guess.

[3] The SANS Institute. "Top Cyber Security Risks", http://www.sans.org/top-cyber-security-risks/.
[4] Garner. "Gartner says companies that don't implement stringent remote worker policies will see remote worker costs increase five to ten times." http://www.gartner.com/it/page.jsp?id=497104
[5] http://www.smeweb.com/management/top-tips/making-remote-working-work-031008.html

Client-side performance

End users have little patience with slow computers, regardless of whether they are on-site or at home in their pyjamas. The industry continues to produce faster processors on a regular basis, and this fuels our expectations for responsive applications. When the computer takes too long to boot, or when an application doesn't respond to a command within a split second, people call the help desk. Or, worse, they disable anti-virus software altogether.

Client-side security has the advantage of performing a final check after traffic has already passed through a corporate firewall, but it often comes with a performance hit. Companies may have dozens of older computers that are still in use, which struggle with resource-intensive client-resident security programs and huge virus definition lists.

Overworked IT staff

Nobody has an unlimited IT budget. This is especially true in entrepreneurial companies where funds are needed for growth. Often, IT staff are overwhelmed with routine technical support and systems administration. Time spent "putting out fires" leaves no time for putting good security practices in place.

In fact, according to the Cybersecurity Watch Survey[6], only 56 percent of respondents actually had a formal plan for managing security and responding to incidents. Nineteen percent said they had no such plans but planned to create them within the next year, and 18% had no plans at all.

As a result, companies need security systems that are as simple as possible – fit-and-forget rather than install-upgrade-and-fidget – and they also need systems that provide the greatest security for the least amount of management oversight. They need a solution that installs endpoint security easily, manages it consistently and keeps it up to date automatically.

The hosted alternative

Hosted services (also known as cloud computing, software-as-a-service or SaaS) are becoming increasingly popular. It requires little or no on-site hardware and companies usually pay for it on a per-user fee. Moving applications and security to the cloud can lower capital costs, make management easier and improve flexibility.

The greatest benefit of hosted services is that it delivers economies of scale and expertise. For example, with hosted security, you get the benefit of IT security experts and robust, up-to-date technology. It is simply too hard and too expensive to build this capability in an individual company.

Besides the human resources, the technology resources are also state-of-the-art. The hosted security provider's data centre is much more likely to possess the latest technology, high-end servers and fast connections, all of which are managed and monitored 24x7.

Other advantages include streamlined management and ease of deployment. With the service provider taking care of routine maintenance, upgrades, security patches and other tasks, the client can focus on other areas of the business. Control and visibility over the security environment is retained however, with a secure web-based portal that delivers detailed reports and the ability to change policy settings or carry out routine tasks such as adds/changes/moves.

Hosted security's biggest advantage however, is that it solves the remote user dilemma. In-house solutions don't update remote users until they log into the company network. This means delays and vulnerability. In a hosted environment, geography is irrelevant. The solution provider pushes updates to each client automatically, regardless of location.

[6] "2010 Cybersecurity Watch Survey". CSO Magazine.
http://www.csoonline.com/documents/pdfs/2010CyberSecurityResults.pdf

Introducing Symantec Endpoint Protection.cloud

Combining strengths in security and hosted environments, Symantec Endpoint Protection.cloud solves the challenges of PC security.

With no need to install additional hardware or software, Endpoint Protection.cloud secures all PCs, including remote users' notebooks and desktops, with complete security that includes antivirus, antispyware, firewall, intrusion prevention, and web browser security. Benefits include:

- **Online management.** Administrators have access to a web-based management console for easy access to common functions, and full visibility and reporting.
- **Easy client deployment.** Client deployment is transparent and automatic. Every client, regardless of location, is assured of having the latest updates at all times.
- **Security expertise.** Endpoint Protection.cloud brings together Symantec.cloud's decades of experience fighting online crime and malware and combines it with Symantec.cloud's heritage of hosted security software and online management.
- **No trade-off between accuracy and complexity.** Endpoint Protection.cloud offers a combination of ease of use and complete service.
- **Predictable costs.** Managers no longer have to worry about capital costs for security, expensive licensing fees and high manpower costs. Endpoint Protection.cloud comes with an affordable, predictable subscription fee.
- **Scalablity.** The service is easily scalable, allowing a company to easily add on new endpoints as needed, without having to worry about upgrading to new management software or purchasing additional hardware.

With Symantec.cloud, you enjoy comprehensive protection of all of your endpoints, automatic updates, easy web-based management and instant scalability. Managers and administrators have full visibility into the system and access to customisable reporting, and end users will always have up-to-date protection regardless of location.

Conclusion

Endpoint security has become more complicated and resource-intensive. At the same time, the workforce has become more mobile, which adds synchronisation delays to the traditional model of endpoint security. A cloud model adds a new level of reassurance to IT security by allowing companies of all sizes to gain access to the best equipment and most talented security experts. With Endpoint Protection.cloud, your end users have the state-of-the-art protection they need, all in one easy solution.

About Symantec.cloud

Symantec.cloud is a leading provider of hosted messaging and web security services, with over 30,000 clients ranging from small businesses to the Fortune 500, located in over 100 countries. Our services protect, control, encrypt and archive communications across email, web and instant messaging. These services are delivered by a globally distributed infrastructure and supported 24/7 by our security experts. This gives a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information. For more information or to request a free trial of our services, please visit www.messagelabs.co.uk.

More Information

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

CANADA
170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

BELGIUM/LUXEMBOURG
Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

DACH
Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

NORDICS
St. Kongensgade 128
1264 Copenhagen K
Danmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +44 (0)870 850 3014

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

1/2011 21167340