WHITE PAPER: 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.

A Whitepaper by Symantec.cloud

Symantec.cloud

White Paper: Endpoint Security

Meeting the Challenges of Endpoint Security

Contents

Introduction 1

Complacency and Risk 1

Business Challenges 1

The Threats Keep Coming 2

Protecting Mobile Users 2

Client-side Performance 3

Overworked IT Staff 3

The Cloud Alternative 3

Introducing Symantec Endpoint Protection.cloud 4

Conclusion 5

More Information 6

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 unauthorized 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 workforce:** The increase in flexible and mobile workers have 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 defense against security threats backed up by in-house security expertise. When you multiply best-of-breed point solutions for security what you get 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 sense of security. They think they are safe, but they're not.

Business Challenges

Companies are facing 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-http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html

- **Ad-hoc PC management.** Growing companies often have limited or non-existent PC management systems. This makes it harder to ensure that software installations and PC configurations are consistent and it 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 administration 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 defense 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 Research, companies that do not address mobile security risks properly will experience more security breaches and this will increase the costs per remote worker 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. Worldwide, more and more companies provide tele-work 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, control over it, check how up to date the security software is, and monitor what websites 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

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

installation of unauthorized 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.

Client-side Performance

End users have little patience with slow computers, regardless of whether they are on-site or at home in their pajamas. 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 – "set-it and forget it" 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 Cloud Alternative

Cloud services (also known as hosted services, 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 cloud services is that it delivers economies of scale and expertise. For example, with cloud based 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 cloud security provider's data center is much more likely to possess the latest technology, high-end servers and fast connections, all of which are managed and monitored 24x7x365.

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.

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

Control and visibility over the security environment is retained 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.

However, cloud security's biggest advantage is that it solves the remote user dilemma. Many 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. Each client automatically obtains updates directly from the cloud solution provider, regardless of location.

Introducing Symantec Endpoint Protection.cloud

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

With no need to install any management hardware or software, Symantec 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.** Symantec Endpoint Protection.cloud brings together Symantec's decades of experience fighting online crime and malware and combines it with MessageLabs' heritage of hosted security software and online management.
- **No trade-off between accuracy and complexity.** Symantec 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. Symantec Endpoint Protection.cloud comes with an affordable, predictable subscription fee.
- **Scalablity.** The service is scalable, allowing a company to easily add on new endpoints as needed, even in new locations, without having to worry about upgrading to new management software or purchasing additional hardware.

With Symantec.cloud technology, 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 customizable 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 synchronization 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 Symantec 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 uses the power of cloud computing to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging. Building on the foundation of MessageLabs market leading software-as-a-service (SaaS) offerings and proven Symantec technologies, Symantec.cloud provides essential protection while virtually eliminating the need to manage hardware and software on site.

More than ten million end users at more than 31,000 organizations ranging from small businesses to the Fortune 500 use Symantec.cloud to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging.

Symantec.cloud helps IT executives to protect information more completely, manage technology more effectively, and rapidly respond to the needs of their business.

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

Symantec.cloud North America
512 7th Ave.
6th Floor
New York, NY 10018 USA
1 (646) 519 8100
1 (866) 460 0000
www.MessageLabs.com

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.

1/2011 21167364