WHITEPAPER

INFORMATION SECURITY

IT SECURITY

A STEP BY STEP GUIDE FOR GROWING BUSINESSES

STAGE 1: THE SECURITY ESSENTIALS

AUTHOR: DR. JOHN LEACH, SECURITY RISK CONSULTANT

www.jlis.co.uk
john.leach@jlis.co.uk

ABOUT THE AUTHOR

John Leach has been an Information Risk and Security professional for more than 20 years. He has held senior positions in the security teams of several organisations, including NatWest Bank, and has directed the security teams of a number of boutique technical consultancies. In December 2002, he formed his own company to enable him to provide consultancy services independently.

John Leach has an academic scientific training. Many of the services he provides build on his ability to analyse security data, model the dynamics behind security risk, and quantify how the countermeasures people apply measurably reduce the security risks they face. He has been an active member of the Management Committee for the Information Assurance Advisory Council (www.iaac.org.uk) continuously since May 2002, and is a member of the International Board of Referees for *Computers and Security*.

This paper would not have been so well informed as to the profile of today's threats without the assistance of Symantec Hosted Services and the global threat data they provide through MessageLabs Intelligence. Given the nature of its hosted services, Symantec is in an excellent position to capture an enormous amount of homogeneous data about internet-borne security threats. This huge volume of clean data can be used to generate valuable security insights, objective insights based on hard data rather than the more subjective insights, usually based on small-sample surveys or averages across widely diverse data, to which we are normally limited. I am grateful to Symantec Hosted Services for allowing me access to their MessageLabs Intelligence data while I was writing this paper.

Dr John Leach

www.jlis.co.uk
john.leach@jlis.co.uk

MANAGEMENT OVERVIEW

Most SMBs find that their security needs are not well catered for by the marketplace. There is ample detailed technical security advice available for large enterprises with deep pockets and the need for their security to be comprehensive. However, organisations with more limited needs and resources often find it hard to find guidance on what to prioritise and where to draw the line. If they are to stop short of trying to do everything contained in the security pantheon that their larger brethren might take on, then what security controls do they discard? And doesn't that make them hostage to fortune, open to accusations in retrospect that they had fallen short on their security duties if the organisation ever gets hit by a security problem?

This White Paper has been written for those organisations that do not have deep pockets. It sets out a flexible three stage approach that helps organisations sort out what their security priorities should be. It sets out a baseline of security controls that all organisations should apply, and shows how they can build on that baseline, maximising the security protection they can gain from each additional security step taken. Each organisation can set the height of its security bar at the level that is right for it today, and can raise that bar if it needs to as their business grows and their security needs evolve.

INTRODUCTION

Security can sometimes seem like a never ending road. Every IT Manager knows that they need to go some way down that road, that they can't ignore security entirely. But, at the same time, they know that they will never be able to do everything conceivable to eliminate every security risk. They have to draw a line somewhere. But where?

There is an enormous amount of specialist advice available to those who want it from all across the Internet. But most of that advice seems to be aimed at persuading large organisations to find yet more budget and resources to do even more of the things that they are not yet doing. Where does this leave everyone else, especially those IT Managers who don't have deep pockets and whose security needs are not so comprehensive? They still want to be able to assure their Managing Directors that the limited amount of time and effort they are able to spend on security is being put to proper use. They want confidence that they are doing all the security things that they really should be doing. At the same time, they don't want to be wasting their efforts on things that are in any way unnecessary. And they need security to be easy to understand, maintain and manage. Anything else leads to a waste of time and money and reduces the return they get for all their hard work.

Security might seem like a never ending road but that does not mean that an IT Manager is failing to take their security responsibilities seriously if they decide it is not possible for them to do everything there is to. Managing security risk is about drawing the line in a sensible place. It is about doing enough not to leave the organisation wide open, but not so much that money and effort is being spent on things that give only a small return.

For some SMBs, that will mean doing much less than others are doing. Some SMBs will never have the time and resources, or indeed the security need, to do more than just the essential security basics. That could well be the right choice, provided the organisation's needs are limited and provided it does those security basics well.

For other organisations, it might mean doing much more than others are doing. For large organisations, the security road can become a four lane highway with all manner of security activities taking place. These organisations will be doing risk assessments of individual key systems and building their own bespoke security solutions, protecting themselves through 'defence in depth'. There will always be plenty of things they could do to keep themselves highly secure.

The vast majority of organisations, and probably every SMB, will find it needs to draw the line somewhere in between. This paper has been written for that majority. It describes three stages of development along the security risk management path, starting at the beginning.

- **Stage 1** – do the security essentials. Every organisation should implement at least this minimum set of security controls to give themselves a baseline level of protection. This paper will say what these basic security controls are. Every organisation, no matter how small, should at least make sure it gets through to the end of Stage 1.

- **Stage 2** – customise the essentials. Before trying to take on a wider range of security controls, customise those basic security controls to maximise the return they provide. This paper will describe how to do that. Every organisation should make a start on this second stage, even if it decides not to make it through to the end.

- **Stage 3** – fill in some of the gaps. For those who still have some fuel in the tank, identify where there is a mismatch between security need and security provision and start to fill in the gaps. This paper will show how to go about that.

This three stage approach has flexibility. It recognises that no two SMBs have exactly the same needs and that one of the characteristics of SMBs is that they can grow and change rapidly. This three stage approach allows each organisation to find the level of security that is right for it today, and then, when it is ready, to build on that level, raising its security bar and adding to its security efforts efficiently, bit by bit as it grows.

This White Paper is in three parts. Part 1 describes the threat landscape as seen by SMBs, and describes the security controls that belong in Stage 1. Part 2 describes how organisations can develop a security profile for themselves that will show them which of the Stage 1 controls they most need to build up and strengthen. It then describes how to do that strengthening of each of those Stage 1 controls. Part 3 describes how to move on from the basic controls and how each organisation should decide which, of all the many tens of extra security controls available, are right to be brought in next.

All three parts of this White Paper can be obtained from www.messagelabs.com/essentials

SETTING THE SECURITY CONTEXT

Many IT Managers will say "I don't need to know about the threats, just tell me what I need to do." That is a sensible approach, and this paper will tell those IT Managers everything they need to do. But even so, it helps if people can have a general idea of what they need to protect themselves against, because that provides the context for all the basic security things that need to be done. It helps make security make sense. So we will start with that.

Sifting through the overload of information about all the security threats that are out there, and disregarding the fact that there will always be someone who will say that this or that additional threat is simply the most important and mustn't be ignored, the following are the six top things SMBs need to protect themselves against.

- Accidental systems failure
- Malware
- Malicious web sites
- Untargeted attacks by outsiders
- Rogue employees (including those just about to leave the organisation who want to take some useful data with them)
- Careless or inattentive employees

We will take a brief look at each of these so people can get a good idea of what they are dealing with.

ACCIDENTAL SYSTEMS FAILURE

Everyone will know what this one looks like. Some piece of equipment breaks, some essential service goes down. It's immediately disruptive. And unless it affects only some component that is not critical to the business, it has to be dealt with straight away. Most SMBs do not have a large stock of spares on standby and are not able to dual source essential services. So what do they do? They hunt for a spare and if they don't have one they race out and get one from a suitable supplier. They make lots of telephone calls trying to get action as swiftly as they can. And they make do the best they can in the mean time.

We'll say no more about this one here as it is not part of the main focus of this paper, other than to say:

- Keep a spare or two of any equipment that is truly essential;
- Try to stay on good terms with your suppliers so they help you out when you need them to.
- Try to keep staff on side so they pitch in and pull together when you need them to.

MALWARE

Malware includes a wide variety of malicious traffic, mostly email but IM (Instant Messenger) traffic too, that, on the whole, is designed to get unauthorised software onto vulnerable machines, most often to conscript those machines into a botnet or to steal passwords or files.

The following malware insights have come from an analysis of some of MessageLabs Intelligence data for December 2009[1].

- Most of the malware an SMB is exposed to (50% - 55%) is phish. Whilst phish is primarily a threat to people's personal banking accounts, it can also be a threat to the organisation's accounts (financial accounts and system access accounts).
- Malware containing malicious links makes up only a small proportion (<10%) of the malware SMBs see. However, this is expected to increase over the coming year, not only because attackers are become more proficient but also because shortened URLs are becoming popular. Because there is no way people can tell where a shortened URL will take them, phishers have started to use these to disguise links that the average security conscious user would not otherwise touch. MessageLabs Intelligence is already seeing an increase in the use of this tactic, and Symantec expects that growth to continue through 2010.
- The rest (malware that is neither phish nor malicious links) encompasses a wide range of malware strains. Its composition varies from month to month and often it is this category of malware that has the greatest potential to cause serious damage. For example, the most common strain in December 09, accounting for around 40% of the total in the one month analysed, was a series of malware campaigns designed to infect users with Zbot. Zbot is a Trojan that secretly installs spy programs and/or keyloggers on people's machines. These then steal banking and/or other personal information.
- As cybercriminals exploit new ways to bypass CAPTCHA[2] technologies, IM is likely to be used increasingly for sending spam messages containing malicious links. Symantec Hosted Sevices reports that, in mid 2009, 1 in 78 IM links were to domains hosting malware[3]. They predict that, by the end of 2010, that will have risen to 1 in 12.

[1]http://www.messagelabs.com/intelligence.aspx
[2]The test sometimes used by web sites to prevent the automated creation of fraudulent user accounts. It is based on deforming the image of a word or sequence of letters in a way that makes the text indecipherable to a computer but not to a human.
[3]http://www.messagelabs.com/intelligence.aspx

MALICIOUS WEB SITES

Web browsing can cause security problems either because the web site being visited was designed to serve up malicious code or because a legitimate web site has been hacked and malicious content uploaded to it. Often, malicious code is hidden within legitimate looking documents that can be downloaded from the site, such as .PDF, .DOC, .XLS, .PPT. The recipient only has to open the file and their computer becomes compromised. Even more difficult for IT Managers to intercept is where the malicious code is downloaded and installed on a victim's vulnerable machine without the user having to do anything more than just visit the infected site. This is sometimes known as "drive-by downloading".

80% of websites blocked for hosting malicious content are well established and over three months old, some as many as ten years old[4]. These are nearly always legitimate sites that have been compromised in some way by hackers exploiting an insecurity on the site. This makes it hard for IT Managers to protect against these sites. Simply warning staff not to go visiting the shadier corners of the web provides no defence against this problem.

Looking at data for the past year shows:

- By far the most common category of malicious URLs, about 50% of the total, is advertising pop-ups. Adverts are the most common way unsuspecting users are lured into downloading malicious code.
- Of the rest, a significant proportion of URLs serving up malicious content are ones associated with legitimate business sites, the type of sites that staff might well go to as they go about their work (computing sites, Internet blogs and forums, reference sites, and other business related sites).
- The next most common group of malicious URLs are what might be classed as personal / social sites, e.g. news, politics, entertainment, fashion, social networking, banking, travel, sports, health, games, cars. Again, it is hard to stop staff visiting these types of site.
- Vice sites (e.g. porn, gambling, hate sites, weapons, criminal, etc.) are relatively unlikely routes for staff to get tricked into downloading malware, not because these sites don't contain their share of malware but because staff visits to these sites while they are at work are normally rare. The visits that are made occur predominantly outside normal business hours, peaking in the midnight to 3 AM period.
- Interestingly, another channel that is just starting to be used to trick users into download malicious content lies in the mobile arena: malicious apps for smart phones.

UNTARGETED ATTACKS BY OUTSIDERS

These are manual attacks by hackers (rather than automated attacks by malware) against IT systems, mostly designed to get unauthorised software loaded onto a vulnerable machine so the attacker can gain access to personal or corporate data files.

The objective behind these attacks is usually to steal something. In most cases, it is any corporate information that looks like it might be interesting (which the hacker will steal first and then decide afterwards what use they can make of it). Or, if the attacker has reason to believe that the organisation might be holding data of specific value (such as customer files with credit or bank account information in them), they will be looking for those whilst at the same time being happy to take anything else that looks like it might be interesting.

Targeted, more professionally conducted espionage is rare for most SMBs. In general, it is larger organisations in high value sectors (e.g. finance, petrochemical, pharmaceutical, government) that are the prime targets for this. But, as targeted attacks become easier to perform, they are starting to get directed against a wider range of industries and a wider variety of business sizes. According to MessageLabs Intelligence, exposure still remains low for SMBs below 250 staff, though if the current trend continues, this lower limit will fall. Any SMB that is a likely target for this type of attack will probably know that it is one already.

[4]The results in this section are based on 12 months of MessageLabs Intelligence data, the same data that the MessageLabs Intelligence Reports are based on.

ROGUE EMPLOYEES

This includes staff who are willing to commit theft or fraud, or, more commonly, those just about to leave the organisation who want to take some useful files with them.

Theft and fraud have traditionally been aimed at stealing cash or funds, but increasingly nowadays they are aimed at stealing data. Data theft is an issue for all organisations and can occur using a variety of channels, most commonly email or removable media.

Data theft is not accidental. Staff who take (on pocket-sized removable media) or send (via email to personal accounts) sensitive or valuable data off the premises know perfectly well that they do not have their employer's permission to do so. Most data theft is of proprietary information and the harm it leads to is a loss of business and customers. If the data stolen is personal information relating to customers or staff, the theft could also cause the organisation regulatory compliance problems too.

CARELESS OR INATTENTIVE EMPLOYEES

It is widely said (but remains nonetheless generally true) that the weakest link in the security chain is usually well intentioned but insecure staff.

By far the largest part of this problem comes from staff making avoidable mistakes, errors which lead to laptops and valuable information being lost, stolen or corrupted, or who inadvertently bring infections into the organisation when they should have known better. Anybody can make mistakes; the problem is that some people make mistakes a lot more often than others. Senior staff tend to be no more careful or security aware than junior staff, their avoidable mistakes can be more damaging, and they are usually harder to educate or discipline.

Currently the smaller part of this problem, though this part is growing, comes from what is called social engineering, attackers attempting to trick end users into downloading malware or divulging sensitive information under the belief that they are doing something perfectly innocent. The popularity of social networking has fuelled a growth in social engineering attacks. Social network sites provide an easy means for attackers to gather the sort of information they need if they are to pose as a friend or someone else the end user might trust.

SO WHAT'S TO BE DONE?

Given that that brief foray shows what the general threat landscape looks like today, how should organisations with limited resources go about dealing with these things? As mentioned earlier, there are three stages to the security risk management journey. Every organisation should complete Stage 1, most should be able to get value out of Stage 2, a few will go on to Stage 3 and beyond.

STAGE 1: THE SECURITY ESSENTIALS

The following is my checklist (in no particular order) of the essential security controls every organisation should use to cover the common threats described above. IT Managers should work through this list and make sure every control can be ticked. They shouldn't be daunted by the number of items on the list. Most SMBs will already be doing most of these things. None of these controls is particularly difficult to apply so effort should go into making sure they all get done adequately well. They need no more justification than, say, locking the front door when you leave the house in the morning. They should be looked on as part of the cost of staying in business.

Stage 1: Security Essentials

Do the security basics

- Back-ups
- Anti-spam
- Anti-virus
- Firewalls
- User authentication/ access controls
- Logging
- Patching
- Scans
- Security culture
- AUP
- Zombies

Back-ups

As well as keeping a spare or two of any equipment that is truly essential, back-up your essential systems and data. Enough to rebuild each server or user's desktop if it crashes, or to recover anything that gets lost or damaged from an outage of an essential service. Be clear who has the responsibility of taking the lead whenever there is a need to rebuild or recover.

Anti-spam

Spam would be just an annoyance and a consumer of bandwidth rather than a security concern if it weren't for the fact that spam is the main carrier of malware. Anti-spam filtering is essential, not as an alternative to anti-virus but as a first-pass filter to clear most of the obvious malware out the way. This leaves the anti-virus product to catch the trickier malware.

Any e-mail service provider worth its salt will provide its customers with a decent level of anti-spam filtering. Any organisation running its own e-mail should make sure it has good anti-spam protection in place that blocks spam before it gets on to the network. This can take the form of either a hosted service or a leading commercial anti-spam product that the organisation keeps regularly updated.

Anti-virus

In conjunction with anti-spam, run anti-virus. Statistics[5] still suggest that the use of AV amongst SMBs is less than 100%. There cannot be any good reason not to be using AV protection in the current climate. AV runs in the background, updates itself automatically, and remains all but invisible except for when something malicious gets detected.

Take AV protection seriously. Use either a hosted service or a leading brand commercial product at the network perimeter, plus AV on each desktop. Do not settle for some freebie product off the back of a cereal packet.

Firewalls

Use a commercial-grade firewall at the perimeter, and the O/S-embedded one on each desktop. As with AV, there cannot be any good reason not to have firewall protection in the current climate. Use firewalling to blacklist or block inappropriate sites and suspicious types of traffic (such as external sites trying to push downloads onto your machines).

User authentication and access controls

Sensible passwords[6] will stop most unauthorised use of machines or accounts. And there is no need to force people to change their passwords every month. A good password well looked after can remain safe for a year.

For shared systems, use access controls to prevent abuse, and log the accesses made just in case one day you need to investigate a problem. Without making a big deal of it, make sure staff know accesses are being logged.

Logging

As well as logging system accesses, log outbound data flows (and tell staff you are doing that). Look through the logs periodically just in case they are recording something amiss.

[5]For example, the Information Security Breaches Survey 2008 statistics for UK SMBs
[6]The easiest way I know to create a sensibly strong password is to make it up from two or more short (4 or 5 letter) words that are unrelated to each other. That makes it easy to create and remember long (8 or more letter) passwords that are relatively resistant to most guessing and cracking attempts.

Patching

Apply all patches on a regular monthly cycle. Software vulnerabilities have long been an endemic source of security problems and the level of exploits is not waning. Patching has reached a level of maturity where a lot of the work can be automated. But not all of it. You do still need to think about patching, it isn't yet something that can be set up to run in the background and forgotten.

Vulnerabilities get exploited wherever they are to be found. According to Alan Paller, the head of SANS[7], the vast majority of successful attacks these days are not against operating systems, they are against common client-side office applications such as document management products and media players. Ensure that applications (office and business systems), not just operating systems, get patched.

SMBs, just as much as large organisations, need to keep track of vulnerabilities as they get discovered and of patches as they are released. The SANS @Risk mailings are good for this.

Scans

Scan your systems periodically (say, every three months). Scan for vulnerabilities (in configurations and software) and for unauthorised software (not just malware but any programme or utility that hasn't been explicitly approved by the IT Manager).

Fix the vulnerabilities you find. If they can't be fixed straight away then develop an action plan, don't just leave them for later.

Any software found that shouldn't be there, ask how it got there and what the purpose was. Maybe there is a good reason for allowing it to stay. If you can, prevent general staff from being able to install / permit the installation of ad-hoc software onto their machines.

[7]www.sans.org

Build a security culture

This can be the hardest item in the list. Try to get staff to think of security much as they do Health and Safety. Making sure security accidents or bad things don't happen is as much their individual responsibility as it is the organisation's responsibility. They need to apply common sense in all the day-to-day situations that arise just as the organisation needs to develop the right policies and solutions.

Make security a team thing, something everybody does to help and protect everybody else who works there. Everyone (and that includes the MD equally) shares the responsibility of keeping the organisation's systems and data safe. Talk about security, including both the organisation's successes and its failures. Make it a routine topic of interest rather than something that is never mentioned unless there is bad news.

Acceptable Use Policy

An AUP (Acceptable Use Policy) is essential as much to manage the organisation's liability as it is to improve its security. It is important that the policy is worded the right way and covers all the key points. There are free templates available over the Internet that can provide a good starting point for writing policies, and good guides available on making sure all the key points get covered[8].

Point out to staff that when they are using the organisation's computers, they really do need to stay alert and be careful, for their own sake as well as for the organisation's sake. They need to be especially careful with regard to what comes in via e-mail, and not to follow suspect links, or open any attachments, or say Yes when their machine asks their permission to run or install something, unless they are comfortable they could explain why they did so to the IT Manager. Make sure all staff are aware that malicious code can be buried inside all sorts of files these days, not just .exe files. Make sure any staff who know any of the organisation's financial account access information are especially careful.

[8]For example, www.messagelabs.co.uk/whitepaper/AUP_Practical_Guide_UK.pdf

Clean up any botnet zombies

Most of the millions of zombie machines in existence at any one time are residential PCs, but the contribution from SMBs is probably significant.

Work out if any of the organisation's machines have been recruited into a botnet and clean them up.
The most common way to detect a zombie once it is active is through the spam it sends out. That spam is likely to get detected downstream. Ideally, the organisation will get told about this by its ISP. Often, the sending IP address simply gets blacklisted. Blacklisting impairs the organisation's ability to send legitimate e-mail properly so it should become aware of this quickly enough if it happens.

A more direct way to detect botnet activity from within a private network is to block port 25. Port 25 is the one many bots use to send spam directly out into the internet, avoiding having to send the spam through the organisation's designated mail server. By monitoring attempts to send mail via port 25, an organisation will notice straight away if any of its machines is acting like a zombie. It can then clean the zombie up.

Even if the active zombie doesn't lead to legitimate e-mail being blacklisted, it is still well worth the effort of identifying and cleaning up any zombies the organisation might have.

- Zombies consume resources, so cleaning them up will improve IT utilisation and ultimately save the organisation money.
- Zombies create back doors into the organisation's network, so cleaning them up will help the organisation keep control of its kit.
- Each zombie contributes to the global botnet and spam problem that every Internet-connected organisation labours under. Owners have a duty to everyone else to clean up any zombies they hold and to do their bit to reduce this global problem.

Many ISPs could do a better job of monitoring their customers' traffic and informing customers who seem to have been infected. Each organisation should talk to its ISP and ask to be notified if spam is detected originating from any of its IP addresses. Where possible, block outbound port 25 e-mail traffic, or ask your ISP to block it for you.

Put together a plan for cleaning up zombies so you are properly prepared should any be detected. And when running your periodic system scans, look out for unauthorised software that would indicate a machine has been recruited to a botnet.

STAGE 1: WRAP UP

That concludes the list of Stage 1 essentials, the security controls that every organisation should have in place if they want to take security seriously. As mentioned earlier, for all of these Stage 1 security controls, the key is make sure they are being done effectively. It is more important to get a good foundation in place for the end of Stage 1 than it is to rush on to the next stage, especially as Stage 2 builds on this foundation. Put all of these basic security measures in place. Then, once they have been running a while and are bedded in, work through the list again and check that everything on the list is being done the way it should be. Try to get to where they are all being done reliably and as a matter of routine.

NEXT STEPS – MOVING ON TO STAGE 2

Part 2 of our guide to IT Security describes how organisations can develop a security profile for themselves that will show them which of the Stage 1 controls they most need to build up and strengthen. You can download the Stage 2 work book from www.messagelabs.co.uk/essentials

HOW SYMANTEC HOSTED SERVICES CAN HELP WITH YOUR SECURITY ESSENTIALS:

Symantec Hosted Services, 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 99 countries.

Our core offering is MessageLabs Security Safeguard, an integrated service which combines email security with web and IM protection. All-round defences like this have significant benefits:

- Cost effective security across email, web and IM from a single supplier, with full 24/7 support
- Protection against new and emerging threats, 'in the cloud' before they even enter your network
- Policies applied across email, web and IM to prevent IT misuse and enforce acceptable use
- Unrivalled spam & virus capture rates
- Quick and easy set-up

We secure more than 3 billion email connections and one billion web requests every day for businesses all over the world. As the leading provider of hosted security services, we are likely to see emerging threats soonest.

MessageLabs Security Safeguard runs in our data centres, so it doesn't require lots of expensive capital equipment on your premises. We take care of maintenance, availability, updates and patches, and provide full 24/7 support to all our customers, no matter how big or small they are.

Our approach makes it easy for us to support multiple offices and remote users. It also means that internet criminals can't download our software and use it to test their malware. It's an integrated solution from a single supplier which gives you easier management, a single management console, better reporting and economies of scale.

You can trial our service for free – simply visit www.messagelabs.co.uk/trials/web_smb

>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
Support: +44 (0) 1452 627 766

>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

>NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 1452 627 766

>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

>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

>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

symantec™

Confidence in a connected world.