

The Real Cost of Email Security

Kaspersky[®] Hosted Security Services

Securing email systems against attacks requires considerable resources – both human and financial. The true costs often remain unclear, as few organisations actually carry out a Total Cost of Ownership analysis. This type of analysis, however, frequently demonstrates that appliance-based or other solutions are not as cost-effective as they initially appear. This white paper uses TCO comparisons to demonstrate how organisations of different sizes can realise considerable savings by using an offering such as Kaspersky[®] Hosted Security Services.

Why Email Security?

Recent developments including the trend towards attacks using targeted zero-day – and even zero-hour – exploits mean that corporate security professionals now face considerable challenges. As many of these attacks are designed specifically to circumvent standard security solutions, it is not enough to install a security appliance or server-based solution and to rely on automatic updates for protection. Although this type of solution can be very effective at blocking known exploits, additional defences are required to protect against today's threats. These often have to be developed in-house and implemented immediately. Security personnel have to keep up with the latest threats and attack vectors, checking for updates not just daily, but hourly: a time consuming and costly process.

Another major concern is the continued flood of spam which consumes costly resources and reduces employee productivity. And spam may act as a carrier for malicious programs. In many companies, spam now makes up considerably more than 70% of all emails received, and frequently more than 90%. The German Federal Office for Information Security (BSI) estimates that companies incur costs of up to 7-13 pence for each spam email they receive. Other organisations, such as IDC, estimate this figure to be five times this amount. Even at a very conservative estimate, a company with 500 employees receiving just 10 spam emails a day would incur costs of £380 + a day – or around £140,000 a year.

While most companies have business critical protection for their email systems in place, protection comes at a price. The obvious costs of hardware and software are just the tip of the iceberg. The costs of employing the specialist staff required to manage and maintain these solutions can often amount to many times the purchase price of the solution. It is, therefore, essential to carry out a detailed TCO (Total Cost of Ownership) analysis to calculate all costs incurred throughout the lifecycle of a solution.

Hosted Service vs. Appliance

Kaspersky Lab offers an alternative to the costly in-house implementation and operation of email security solutions – Kaspersky[®] Hosted Security Services. The underlying principle is simple: all emails addressed to a company's employees are routed through purpose-built data centres, where they are scanned for malicious or unwanted content. In this way, spam, viruses, Trojans and other malicious code are filtered out in the cloud, before they ever reach the corporate network. Kaspersky Lab personnel work around the clock to ensure the service is able to combat the very latest threats effectively. Kaspersky[®] Hosted Security Services are fully redundant and highly available – something which is very difficult for companies to achieve in-house.

Compared to an in-house solution, which must be planned, installed and operated by the company itself, hosted security services offer a number of advantages. The fact that Kaspersky Lab operates and updates the service enables companies to realise considerable cost savings on operation and maintenance, as well as on training in-house IT staff. Companies also benefit from an increased and guaranteed level of protection; as Kaspersky Lab is a dedicated service provider, we can implement a wider range of solutions than an individual company. The large volume of email traffic filtered also provides Kaspersky Lab security specialists with a large statistical database. This provides rapid insights into new threats, making it possible to close the window of risk faster and more effectively than an individual company is capable of doing. Even medium-sized companies can benefit considerably from these economies of scale by taking advantage of corporate-level security solutions at SMB prices.

The following sections use typical installations in three sample companies to compare the costs of an in-house email security system with those of using Kaspersky Hosted Email Security. The figures used in the TCO calculations are taken from genuine cases, with a life cycle based on a standard three year depreciation period.

The Cost of Email Security

The cost of purchasing, implementing, managing and maintaining an email security system is made up of a number of different elements. While some of these are obvious, many

Hardware and Software

When implementing an in-house solution, investment in hardware, operating systems and software licenses is required. Smaller companies tend to use appliances with preinstalled virus scanners and, perhaps, spam filters. Larger companies typically install higher-performance appliances or commercially-available server systems onto which IT staff install appropriate software products. It is also possible to avoid purchasing new hardware altogether by installing antivirus software and spam filters on existing mail servers. However, as this type of software requires considerable server capacity, this is a realistic option only for mail servers with a high level of available capacity. Such solutions will require investment for server upgrades, such as extra RAM or larger hard drives.

As well as one-off purchasing costs, the – usually annual – renewal and upgrade costs, as well as vendor technical support must also be taken into account. As a general rule, these expenses equate to around 20% of the initial acquisition cost each year.

Hosted security services require no initial investment, as the entire infrastructure is housed in the provider's data centre. There are no software subscription costs. Instead, companies pay a fixed annual fee for the service. The fee is calculated according to the number of email accounts to be protected.

Installation, Integration and Configuration

Security appliances are end-to-end solutions whereby both the operating system and the security software are preinstalled. As with a hosted security service like Kaspersky® Email Hosted Security, there are no additional installation costs. This is not the case with commercially-available multipurpose servers, where both the operating system and security software have to be installed, and the associated 'platform hardening' process is both essential and time-consuming. This process involves removing all services not required in a security platform to prevent them from becoming potential targets for attack. As doing this requires highly specialised knowledge, the hardening process is not something which can be performed by an inexperienced administrator. Companies whose in-house staff do not have the requisite knowledge may have to call in an external consultant.

Even integrating a security solution into an existing infrastructure has costs associated with it, mainly due to the time spent by the IT department on installation. This involves modifying the settings of other infrastructure components, re-routing traffic, modifying Mail Exchange (MX) records in the DNS system where applicable, etc. These activities must be performed for both product-based solutions and hosted services. Smaller companies without in-house experts often employ an external consultant or a systems vendor to perform these tasks.

Regardless of the approach employed, every company incurs the costs involved in the final configuration of the solution. This is the phase during which a company's security policies are modelled in the system, and

involves defining the spam filter's sensitivity level and deciding how to handle infected or suspicious emails. It also involves creating or importing blacklists and whitelists – lists of addresses or domains from which emails are always blocked or accepted. The more complex the security policy, the more complicated the configuration process. While smaller companies often implement just one ruleset for all employees, larger organisations usually assign different rules to different user groups. Solutions must then be configured to reflect these rule sets.

Ongoing Operation and Maintenance Costs

An extremely important, but often neglected, factor is the personnel costs involved in maintaining and ensuring the smooth running of a security solution. Throughout the entire life of the solution, both the operating system and the security software must be kept up-to-date by applying patches. As security solutions are mission-critical infrastructure components which must remain operational at all times, these patches have to be tested before being installed. The security software must also be constantly updated to take into account current and emerging threats. While new virus signatures are usually installed automatically and therefore require little in the way of resources, combating spam often requires manual intervention. This includes maintaining blacklists and whitelists, as well as the continuous adjustment of filters in order to block spam more efficiently and to keep incorrect detections to a minimum. The time involved in monitoring the market and threat level and in further training must also be taken into account.

Opting for a hosted service can provide considerable cost savings. Kaspersky® Hosted Email Security runs on Kaspersky Lab infrastructure, while Kaspersky Lab specialists monitor the situation. Company IT staff will be required to make only occasional modifications to their security policies, accounting for around 20% of the total maintenance involved.

Upgrade Costs

While regular software updates and patches are normally covered by subscription fees, major software releases must usually be paid for separately. Companies also have to assume that the volume of email messages – both legitimate and spam – will continue to increase. This may mean that mid-lifespan updates may be required to increase the capacity of hardware that was initially adequate. A comprehensive TCO analysis should factor in around one-sixth of the original purchase price for hardware and software upgrades. New software versions and hardware expansions must also be tested, implemented and put into operation, and the costs of this must also be taken into account. A hosted service such as Kaspersky® Hosted Email Security eliminates these upgrade costs.

Productivity and Helpdesk

An important expense often overlooked is that of the helpdesk. If we assume that every user makes an average of six support calls a year regarding the email system, and that handling each call takes five minutes on average, dealing with such email issues will result in helpdesk costs of around £7.50 per user per year. Similar costs are occurred as a result of related lost productivity. Experience has shown that employing an external managed service to filter spam and malicious code in the cloud can reduce the number of support incidents by around 80%. This is

especially true when users are provided with direct access to their quarantine folders, without the need of involving the helpdesk. Kaspersky® Hosted Email Security provides such direct access.

Bandwidth and Drive Space

A detailed TCO analysis should take into account the cost of bandwidth and hard drive space taken up by malicious code and spam messages. Although disk space is inexpensive compared to acquisition and administration costs, bandwidth costs are considerably more significant. Using an external service can help an organisation retain up to 30% available bandwidth, as filtering takes place on the Kaspersky Lab infrastructure and consequently, spam and malware do not reach a customer's network.

TCO Calculation and Comparison

To effectively compare the total costs of different solutions, all the aforementioned costs should be taken into account. Additional costs, such those of planning and purchasing the solution, and costs incurred at the end of the life cycle, vary according to the type of system selected and can, therefore, be excluded from this TCO comparison. They should, of course, be included in a specific TCO calculation.

The following sections compare TCO calculations for three different corporate structures. The first example concerns a SME enterprise with 200 mail users whose accounts must be protected against spam and malicious code, and compares the cost of an appliance-based solution with that of using Kaspersky Hosted Email Security. This is followed by a similar calculation for a larger company with 2,000 users. The third comparison is also based on a company with 2,000 users, in this case distributed among three different sites.

For 200 Users

A company with 200 email accounts should plan on investing around £2,250 in a security appliance. Depreciation over three years produces an annual charge of £750, ignoring lost interest. Each year, an additional 20% of the initial investment, or £450, will be incurred in subscription costs. These example calculations also take into account the cost of an upgrade (£380) in the second year of operation. Depreciation and subscription costs do not apply when using a service such as Kaspersky® Hosted Email Security, and no upgrades are required. Instead, an annual fee of around £4,500 covers everything.

Around two person days should be estimated for implementing an appliance-based solution (installation, integration and configuration), with an additional half-day for the upgrade during the second year. With Kaspersky® Hosted Email Security, this time is reduced to approximately one half-day, which is required to configure the solution. The only other implementation task involves modifying the MX records to route incoming email to the Kaspersky® Operations Centre.

With a hosted security service, regular maintenance is limited to maintaining the configuration, i.e. modelling corporate security regulations on the solution. Maintaining the filters, blacklists and whitelists will take around 4 person days. With an appliance-based solution, the time involved in updating both the platform

and the security software should also be factored in. As this type of solution presents considerably greater challenges to administrators, significant time for monitoring the threat situation and for further training must also be factored in. All in all, around 20 person days a year should be estimated for maintaining an appliance-based solution.

If we estimate the cost of a person day at £300, it becomes apparent that the administrative costs alone for an appliance-based solution amount to several times the acquisition cost. Helpdesk and support costs, too, must be factored into the calculation. If, as before, we assume annual helpdesk expenses of £7.50 per employee, companies with 200 employees can expect to pay £1,500 a year. Experience has shown that using a hosted service reduces the number of calls by around 80%. Lost productivity must also be taken into account. This amount is roughly the same as that estimated for the provision of technical support. As IT specialists generally command above-average salaries, however, the figure used in the sample calculation equates to 80% of the support costs.

Providing broadband Internet access to 200 users currently costs around £3,800. The majority of this bandwidth is required for email traffic. At spam rates of 70 to 90%, it is therefore reasonable to assume that spam takes up at least 30% of the available bandwidth, costing £1,150. By comparison, the cost of the hard drive space required to accommodate this volume of email is almost insignificant.

As Kaspersky® Hosted Email Security filters email traffic in the cloud, corporate networks remain free from spam and malicious code. This means that companies require considerably less powerful Internet connections, which are then fully available for use by legitimate, useful data.

These calculations show that using a hosted security service can save a medium-sized company with 200 users around £4,500 a year. This example is not, however, a true like-for-like comparison, as a hosted service like Kaspersky® Hosted Email Security uses redundant technology to ensure continuous uptime, while an appliance represents a single point of failure. Companies wishing to implement more redundant systems will need to invest in a second appliance, thus increasing the administration costs accordingly.

For 2,000 Users

Providing protection for 2,000 email users requires a much higher-performance system than that required for 200 users. Even appliances with just one signature-based virus scanner and one spam filter will easily cost around £12,000, which, with a 3-year useful lifespan, equates to annual depreciation of around £4000. Here too, around 20% of the initial investment amount should be estimated annually for the corresponding support contracts. This equates to subscription costs of £2,400. Expenses of around £6,400 per year are therefore incurred for the security platform alone. These expenses do not include the costs of essential upgrades, or of the in-house or external implementation. A company with 2,000 users should expect this process to take an average of three person days. Running costs should be assessed as involving at least twice as much time as that estimated for the smaller, 200-user solution.

Unlike administration costs, helpdesk costs increase in proportion to the number of users, making this expense more significant for a larger company. The same applies to productivity lost through support calls. As switching to a hosted security service can dramatically reduce the number of support calls, the potential savings in this area are correspondingly large. In even larger environments, with tens of thousands of users, the savings on IT support alone would cover the cost of a hosted service.

While bandwidth costs do not increase proportionally to the number of users, the cost of connecting 2,000 users to the Internet is obviously much higher than that of providing connectivity for just 200. If we assume an annual total cost of £9,400, 30% of which is wasted on spam emails, the potential savings in this area amount to £2,800 per year. Overall, the TCO comparison for 2,000 indicates potential savings of at least £12,000 per year. This figure does not take into account the additional costs of acquiring redundant appliances.

For 2,000 Users Across Three Sites

The discrepancy between appliance-based and service-based security solutions becomes considerably clearer when we look at a company with multiple offices and mail servers. If we assume that the 2000 users from the aforementioned examples are distributed among three company sites, each site will need its own appliance, which must then be installed and maintained. While it is certainly possible to install lower-spec systems at each location than the 2000-user system installed at the main office, the total acquisition costs still increase considerably. The same applies to the bandwidth costs, as all three sites require high-performance Internet connectivity.

Administration costs, too, are much higher for companies with distributed environments and multiple locations. As many administrative tasks can, however, be performed centrally for all locations, the costs do not increase in proportion to the number of installations. Support costs and costs incurred due to lost productivity remain the same, as these factors depend largely on the number of employees and the type of solution.

The cost of implementing an appliance-based security solution in a company with three sites is around one-third higher than supporting the same number of users at a single location. With Kaspersky® Hosted Email Security the number of locations and mail servers makes no difference to the service costs, as these are based solely on the number of users or mailboxes. The administration costs, too, remain the same, as the service can be wholly managed by a centralised IT department.

Conclusions

If we take into account all the factors involved in operating an email security system, the TCO analysis shows that hosted services offer considerable potential for savings. Compared to appliance-based solutions, for example, using hosted security services can save a company with 200 email accounts an estimated £15,000 – or around 50% of the total cost involved in implementing an in-house solution. The potential savings are even higher for larger numbers of users, particularly for companies which operate multiple offices, each with their own mail server. The Kaspersky® Hosted Security Services redundant infrastructure guarantees 99.999% availability, and the additional layer of non-signature-based malware scanners provides enhanced security.

About Kaspersky Lab

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment.

Kaspersky® technology is used worldwide inside the products and services of the industry's leading IT security solution providers, with over 300 million globally protected today. The anti-malware technologies created by Kaspersky Lab offer the highest detection rates for malicious programs with minimal false positives, thus ensuring effective endpoint protection.

During the past decade and a half, the company has led the antivirus industry in innovation, starting with the first

use of external database signatures in 1992, as well as being first to develop and implement heuristic virus analysis and linguistic text analysis. A dedicated malware lab and international team of experts analyses the latest security trends 24/7/365, thus allowing for the industry's fastest response time to emerging threats and enabling the business to be the first to develop new and forward-looking technologies. It is the company's mission to always stay one step ahead of the competition in offering excellence: the best protection possible ensures the Kaspersky Lab product portfolio remains at the vanguard of the market.

In addition to its multi-award-winning solutions, Kaspersky Lab offers its customers a diverse portfolio of additional services, such as customisation to company requirements. We also develop tailor-made anti-malware solutions and provide staff training.

Kaspersky Lab UK Ltd

E1 Atrium
Culham Science Centre
Abingdon, Oxfordshire
OX14 3DB
United Kingdom

www.kaspersky.co.uk
Email:
sales@kaspersky.co.uk
Tel. +44 (0) 870 0113461

Kaspersky Security is a registered
trademark of Kaspersky Lab.

All other names are trademarks of their
respective owners.

© 2008 Kaspersky Lab, Ltd