

# Greater IT Security For Small To Mid-Sized Organisations

## Kaspersky® Hosted Security Services

Unlike very large businesses, most small to mid-sized organisations do not possess the know-how and resources needed to protect themselves effectively against Internet threats. The subject is too complex, security specialists are rare and expensive and, as Internet security is simply not part of such companies' core business, it is often neglected. Outsourcing Internet security is, for an increasing number of small to mid-sized organisations an attractive alternative. With Kaspersky® Hosted Security Services, Kaspersky Lab provides a solution which not only guarantees a higher level of security, but which is also considerably more cost-effective than an in-house, appliance-based solution. This whitepaper illustrates how small to mid-sized organisations can protect themselves effectively against Internet threats, and the benefits this protection can bring.

### Small to Mid-Sized Organisations and IT Security

IT security can be split into two distinct, but equally important, areas. The first covers securing individual systems and infrastructure components within the company's own network; the other involves protecting the entire network against external threats. Internal security is usually provided by mature, easy to manage software, such as Kaspersky® Work Space Security or Kaspersky® Business Space Security, which are installed on file servers, workstations etc. Securing networks against external threats, on the other hand, requires a gateway solution. Over the past few years, appliances with pre-installed virus scanners and spam filters have become much more widespread, and these offer smooth, uncomplicated operation. In addition to the high acquisition costs, however, these appliances require constant maintenance and a level of IT security expertise which is simply not available to many mid-sized organisations.

### Hosted Security Services: Security On The Perimeter

Over the past few years, both the quality and quantity of attacks on corporate networks has steadily increased. The increasing virtualisation of business processes has been accompanied by an increase in the professionalisation and commercialisation of IT threats. Whereas hackers were previously interested in causing maximum damage, their aims today are primarily financial. Sending spam is now a lucrative business; successful phishing attacks provide access to victims' bank accounts, and targeted attacks on corporate IT structures are playing an ever-growing role in corporate and industrial espionage.

The increasing professionalism of attackers has, over the past few years, also led to considerable changes in threat scenarios. The object of today's attacks is no longer to infect as many PCs as possible with worms or viruses in order to achieve media attention and fame. On the contrary: today's attacks are mostly intended to keep the threat hidden for as long as possible and to evade the attention of the antivirus program vendors. The longer these take to react to new threats, the more time the attacker has to ensure that the malicious code reaches its target. Consequently, protecting against zero-day or zero-hour attacks – i.e. attacks containing malicious code which are not yet detected by antivirus solutions – is of increasing importance.

---

Although today's software products and appliances also use heuristic processes to recognise new malicious code, these are capable of analysing just a fraction of the emails a hosted service deals with. In hosted security services data centres, millions of customer emails are scanned every day. It therefore rapidly becomes apparent when an email with an attachment has been distributed on a mass scale via botnets.

It is, however, not just threats which have undergone a shift, the attack vectors have also changed. As almost every company uses antivirus software and emails with known viruses are therefore very easily filtered, attackers are constantly developing new methods. The use of social engineering, for instance, using an innocuous email to lure the recipient to a website containing malicious code, is on the increase. The malicious code is then downloaded from the website together with the visible page contents. Attackers take advantage of the fact that while many companies protect their email systems using antivirus software at the gateway or mail server level, web access is often provided via unsecured proxy servers. More recently, increasingly popular instant messaging services have been used to distribute malware.

While large organisations and concerns usually employ a number of security specialists in their IT departments to protect against these and other threats, small and mid-sized organisations are facing a dilemma. On one hand, their IT departments are mission-critical and must be protected accordingly. On the other hand, however, maintaining the appropriate resources in-house is not economically feasible. Security experts and market researchers therefore assume that over the next few years, more and more SMBs will take advantage of outsourced services like Kaspersky® Hosted Security Services in order to protect their IT systems effectively against the wide range of Internet threats.

## Numerous Advantages over Appliances

The principle behind Kaspersky® Hosted Security Services is impressively simple: All emails, web access and instant messages addressed to a company's employees are routed through Kaspersky Lab's purpose-built data centres, where they are checked for harmful or undesirable content. In this way, spam, viruses, Trojans and other malicious code are filtered out of the data stream in the cloud, before they ever reach the corporate network. The experts at Kaspersky Lab work around the clock to ensure that the security solution is always up-to-date and that it is capable of combating the very latest threats. Compared to an appliance-based solution, which has to be planned, installed and operated by the company itself, Kaspersky® Hosted Security Services offer numerous advantages:

- Fully operated and constantly updated by Kaspersky Lab
- Enhanced security
- Kaspersky® Hosted Security Services are fail-safe and highly-available
- Guaranteed security through Service Level Agreements (SLAs)
- Flexible modelling of in-house security policies
- Cost savings and calculable fixed costs with no initial investment
- Compliance with legislation and regulations is ensured at all times

## Relieving the Burden on IT Staff

The most obvious advantage of using hosted security services is the decreased burden on in-house IT staff. The planning, implementation and, in particular, the maintenance of an in-house appliance-based solution presents tremendous challenges to company employees. Very few manufacturers provide complete solutions which cover all threat scenarios and which are suitable for use with email, web and instant messaging services. While implementing specialised products from different manufacturers, therefore, will certainly enable you to achieve a higher general level of protection, this type of solution also requires a great deal of integration and maintenance and involves managing multiple maintenance and update contracts with different manufacturers.

The rapid evolution of Internet threats means that protecting your IT environment involves more than just implementing a range of different technologies. It also requires wide-ranging, up-to date knowledge and continuous system maintenance. A considerable investment must be made in training in-house IT staff and in monitoring the security situation, not to mention in installing updates and patches. Limited resources means that this is possible only for a very few mid-sized organisations.

Kaspersky® Hosted Security Services relieves your IT department of all these tasks, freeing your IT staff to focus instead on strategic IT and security planning. Outsourcing eliminates the issues associated with integrating, operating and maintaining the technical infrastructure, as all these tasks are performed by Kaspersky Lab.

## Enhanced Security

Kaspersky Lab is a dedicated developer of security solutions and has implemented and integrated all available technologies for securing email, web and instant messaging services as part of its services. This enables Kaspersky Lab's data centres to provide small to mid-sized organisations with the type of IT security infrastructure previously only available to

major corporations. As well as Kaspersky Lab's multi-award-winning solutions, additional software products are used to ensure the greatest possible security. All services benefit from the use of BitHunt, a proprietary malware detection system which analyses and classifies millions of emails every day according to particular characteristics and trends. This technology also makes it possible to identify zero-day attacks which stand-alone appliances do not yet detect. The proprietary nature of this technology has an additional advantage: malware writers are unable to test their "creations" against BitHunt in order to optimise them.

## Redundancy and Availability

In-house security solutions are often based on individual gateway appliances which filter and analyse traffic. These appliances form a single point of failure, and if they malfunction, this affects the availability of the entire solution. Usually this type of solution is configured in such a way that the appliance's failure means that the associated service (email, for example), is simply no longer available. The reasoning behind this is that a temporary disruption in the service is easier to tolerate than its insecure operation. However, the significance of electronic communications in today's business world requires that this type of interruption be kept to an absolute minimum.

	Appliance	Hosted Security
Implementation Time	Medium to long	Very short
Total Cost Of Ownership	Medium to high	Low
Reporting	Poor to good	Very good
24-Hour Support	Additional fee required	Included as standard
Guaranteed Results	No	Yes
Compatible With Existing IT	Uncertain	Yes
Investment Required	Yes	No, running cost only
Security Level	High	Very High
Process-Based Security	Not usually	Yes
Customer Specific Solution	No	No
Eases Load On Gateway	No	Yes
Protects Against DoS Attacks	No	Yes
Scalable	Poor	Very Easy
Specialists Required	Yes	No

In contrast to appliance-based solutions, hosted security services have no single point of failure.

The entire IT infrastructure of Kaspersky Lab's data centres is fully redundant. Even in a disaster scenario, the remaining data centres can immediately take over the tasks ordinarily performed by a missing data centre. Unlike other companies, Kaspersky Lab keeps qualified personnel on hand to immediately resolve any issues that may arise. Kaspersky Lab is therefore in a position to guarantee 99.999% availability for its Hosted Security Services – equivalent to a maximum downtime of around 5 minutes a year. Even with redundant appliances, this level of availability is almost impossible for companies to realise in-house.

Kaspersky® Hosted Security Services can even compensate for the failure of a customer's mail server. If emails can no longer be routed through the server, they are stored in the data centre for up to seven days. The emails are then forwarded to the customer's mail server once it is back online.

## Guaranteed Security through Service Level Agreements

Despite increased investments in people and technology, IT departments in small to medium-sized organisations have difficulty in providing security guarantees. The threats they face are too sophisticated, the tasks too diverse and the resources too scarce. Even manufacturers of appliances do not provide this type of guarantee, as they have no control over their products at customer sites. Kaspersky Lab, on the other hand, provides this type of guarantee for its Hosted Security Services. These guarantees, along with any agreed shortfalls, are enshrined in our Service Level Agreements.

Kaspersky Lab provides the following specific guarantees for its Hosted Security Services:

- 99.999% availability, corresponding to a maximum of around 5 minutes downtime per year
- 100% freedom from viruses for which Kaspersky Lab has had a signature for at least 30 minutes
- A spam detection rate of at least 95%

## Flexible Modelling of In-House IT Security Policies

No two organisations are alike, and every company's expectations of IT security are different. As part of its Hosted Security Services, therefore, Kaspersky Lab provides an easy-to-use secure web portal which enables customers to configure their own services and to implement their existing security policies. This allows customers to decide for themselves how to handle spam, whether virus-infected attachments should be deleted or quarantined, and which websites should be blocked. This ensures that, despite using a standardised infrastructure, each customer is in charge of his or her customised solution at all times.

## Low Costs With No Additional Investment

Financial considerations play an important role in deciding whether to use one or more appliances to create your own security solution or to opt for a hosted service. Implementing an in-house solution requires considerable investment in hardware and in software licensing, as well as involving additional costs for hiring and training new members of staff and for implementing, integrating and maintaining the solution.

In order to ensure that your security systems are as effective in the long run as they were on the day they were installed, companies implementing in-house systems must pay annual software licensing fees, ensure that staff training is up-to-date, and continue to invest in add-on products. In contrast, Kaspersky® Hosted Security Services requires an annual fee calculated according to the number of accounts protected. This fee can be treated as an operating cost. No additional running costs for maintenance, repairs or replacement investments are incurred. This provides a high level of planning stability and predictability. The services are also considerably more scalable than appliances. If additional user accounts need to be protected, the licence is simply adjusted. With hardware solutions, on the other hand, the acquisition of an additional appliance is sometimes necessary. This must then be integrated into the overall solution.

In addition to these direct costs, there are countless other less obvious expenses associated with running an security solution. Using an in-house solution, for example, means that spam and viruses are filtered only once they have already entered the company network. As spam makes up 70% of most companies' email traffic, this can result in additional costs for higher bandwidth, additional processing performance and storage. Filtering out undesirable messages in the cloud, before they reach your network, can significantly reduce costs. The enhanced security also reduces the number of security-related incidents, which usually require costly and time-consuming intervention by IT and user support departments.

Sample calculations show that a company with 200 users can save around £6,300 to £7,500 each year, just by using Kaspersky® Hosted Email Security.

## Legal Compliance

The management teams of many small to medium-sized organisations view IT security purely as a technical issue; one which should be left to the experts. However, there is one aspect, beyond the boundaries of traditional IT issues, that should be directly addressed by management. Many of the measures taken to ensure IT security also touch on fundamental legal issues. Filtering emails or instant messages affects an employee's constitutional rights

(data protection, secrecy of telecommunications). Legislation and regulations on modifying or suppressing messages must also be observed – failure to do so could result in the management team facing prosecution. Planning and configuring an appliance-based solution to ensure that legislation and regulations are adhered to and that employees' rights are safeguarded is not a task to be undertaken lightly; it is essential to involve legal experts. Kaspersky® Hosted Security Services are designed from the ground up to take European legislation and regulations into account and can, therefore, very easily be set up in accordance with legal requirements. Nevertheless, Kaspersky Lab recommends taking legal advice before implementing its services.

## Kaspersky® Hosted Security Services in Detail

Kaspersky® Hosted Security Services protect the most important online communication methods – those used by businesses every day:

- Email
- Internet
- Instant Messaging

Our services provide comprehensive protection against all threats to which these services are vulnerable. These include:

- Infection through viruses and other malicious code
- Espionage using Trojans
- Spam
- Phishing attacks
- Transmission of confidential data by employees

## Increased Email Security with Kaspersky® Hosted Email Security

Kaspersky® Hosted Email Security is the Kaspersky Service for securing all of a company's email traffic. The service is based on the popular security software developed by Kaspersky Lab over the last ten years. The company's products are today among the most widely distributed security solutions on the market. Additional software products are also integrated as part of the service to further enhance the level of security. The service draws on the expertise of the multinational virus analyst team headed by Eugene Kaspersky, one of the world's leading experts in the field of malware research.

Kaspersky® Hosted Email Security comprises the components Kaspersky® Hosted Email Security for AV (Anti-Virus) for the identification and filtering of harmful code, and AS (Anti-Spam), which protects user mailboxes against the flood of unsolicited messages. These two components are located

in the Kaspersky Lab data centre, and are completely transparent from a user's perspective. Administrators can use the Kaspersky® Hosted Security Web Portal to easily configure Kaspersky® Hosted Email Security in accordance with their corporate security policies and guidelines.

Kaspersky® Hosted Email Security is based on a very simple principle. All incoming and – if desired – all outgoing email is analysed and classified at the Kaspersky Lab data centre. Legitimate email, i.e. those which do not contain malware or are not classified as spam, are then forwarded to the intended recipient within seconds.

If, on the other hand, an email contains malicious code, it is usually – depending on the customer's security policy – deleted or stored in an area of the data centre infrastructure accessible only by an administrator. Kaspersky Lab's BitHunt technology uses heuristics to detect even zero-hour threats, and suspicious emails can be quarantined until a signature for the new malware has been created.

While harmful software can be reliably identified as malicious, spam can be more difficult to classify. Many messages, such as newsletters, may be viewed by some recipients as spam, while for others they contain valuable information. This makes spam very difficult to identify with complete certainty.

In order to make this classification as accurate as possible, however, Kaspersky® Hosted Email Security uses a combination of all the spam recognition techniques. Administrators can also create blacklists and whitelists of domains, resulting in no email – or all email – being accepted from these domains. Once an email has been scanned using Kaspersky Lab's multiple detection and classification techniques, it will be flagged using a probability rating.

If an incoming email is classified as spam, it can be flagged as such and forwarded, deleted or placed into the intended recipient's personal quarantine folder. This quarantine folder is stored on the data centre infrastructure and can be accessed only by the individual concerned, who is kept up-to-date concerning the contents of their quarantine folder via regular, configurable reports. This prevents spam emails from reaching the corporate network, while ensuring that legitimate emails which have been incorrectly classified as spam (false positives) are not lost. After a retention period defined by the administrator, usually 30 to 60 days, the messages are automatically deleted from the quarantine folder.

Setting up Kaspersky® Hosted Email Security is extremely easy. It involves modifying the domain's MX record to point to the Kaspersky Lab data centre. This task can be performed by any experienced administrator in just a few minutes.

## Kaspersky® Hosted Web Security Protects Internet Access

Just as Kaspersky® Hosted Email Security AV protects companies against malware transmitted via email, the Kaspersky® Hosted Web Security service secures the often neglected aspect of Internet access. Many companies access the Internet via insecure proxy servers. Kaspersky® Hosted Web Security also acts as a proxy, meaning that all websites accessed by company employees are first routed to the systems in the Kaspersky Lab data centre. Here, the associated pages are called up and the data stream, including all downloaded scripts, files or macros, is checked for harmful code and spyware before being routed back to the company's employees. Only streaming media content and encrypted data traffic (HTTPS/SSL) cannot be scanned. The entire process is fully transparent for the user and the diversion and scanning processes take a matter of milliseconds, making the delay almost imperceptible.

Administrators can define user messages to inform users whenever a virus or spyware is detected.

## Protection From Undesirable Content

Additionally, the Kaspersky® Hosted Web Security service enables companies to restrict access to the Internet and to prevent access to undesirable websites and content. Administrators can use the service portal to select the website categories and content types to which access should be blocked. Alternatively, Internet access can also be restricted to websites specified in a positive list. It is also possible to create user groups for which specific access guidelines can be defined.

When a user calls up a website or an attachment which is subject to access restrictions, access to the site or attachment is denied, and a warning page is displayed or a warning email sent.

In addition to placing restrictions on certain site categories and content types, Kaspersky® Hosted Web Security also enables schedules and quotas to be set for incoming and outgoing traffic.

## Kaspersky® Hosted IM Security for Secure Instant Messaging

As with Kaspersky® Hosted Web Security, Kaspersky® Hosted IM Security acts as a type of proxy – in this case for the instant messaging services used by the company. Here, too, all traffic is routed through the Kaspersky Lab data centre, where viruses and spyware are filtered out. It is also possible to create dictionaries or word lists to enable messages containing particular words to be blocked. Administrators can define user messages to inform users of the discovery of a virus or spyware.

If a company wants to permit only certain instant messaging applications, undesirable applications can be blocked. This also applies for add-on services, such as video, games or voice applications. Kaspersky® Hosted IM Security also allows administrators to set up different rules for specific user groups, enabling different policies to be implemented.

## Everything Under Control

The principle behind Kaspersky® Hosted Security Services is that in spite of outsourcing, customers retain control of their own security policies and guidelines. Administrators can use the service's secure web portal to implement new rules or modify existing ones at any time. The portal can also be used to define the type and frequency of automatic reporting. The service can provide a variety of reports showing different levels of detail. These reports are created automatically and emailed to administrators at selected intervals and in their choice of format (including graphical, XML, PDF, CSV or table). These reports provide administrators with information about blocked emails and any malware, spyware, phishing attempts, etc, that have been detected. They can be broken down into individual domains, user groups and users and customised for specific time frames. This enables administrators to easily monitor the service levels guaranteed by the SLAs.

---

## 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](http://www.kaspersky.co.uk)  
Email:  
[info@kasperskylab.co.uk](mailto:info@kasperskylab.co.uk)  
Tel. +44 (0)871 789 1632

© 2008 Kaspersky Lab Ltd.

Kaspersky, Kaspersky Anti-Virus logo and Kaspersky Lab logo are registered trademarks of Kaspersky Lab Ltd.

All other names and trademarks are the copyrighted work of their respective owners.