



SoftScan email security service

External spam and virus filtering – on your terms

Spam and viruses are a considerable problem for organisations that receive thousands of harmful and unwanted emails everyday. Today, spam accounts for 90-95% of all emails and viruses less than 1%. With external email scanning from SoftScan you can forget all about spam and viruses, and concentrate on tasks that will add value to your business.

SoftScan's email security service provides you with several benefits:

- **Total email security:** SoftScan protects both inbound and outbound email traffic.
- **Resource saving:** No investment for installation or maintenance of hardware and software is required, including the updating of spam and virus software.
- **Less bandwidth:** SoftScan removes spam and viruses, so only legitimate emails are sent to your internal mail server.
- **Additional backup:** If SoftScan cannot contact your mail server, you are immediately notified and all emails are queued on SoftScans' servers for up to 7 days.
- **Easy administration:** The web based administration console provides a general overview of an organisation's email traffic and allows you to easily setup rules, manage emails in quarantine etc.
- **Additional network protection:** Protect your own servers against internet spammers by setting them to only recognise SoftScan's MX record.
- **Guarantee:** SoftScan's Service Level Agreement (SLA) ensures a high level of service is always provided, in terms of both support and functionality. The solution has also been certified "Checkmark Premium Anti-Spam" by independent testers at West Coast Labs in November 2006.
- **Free support:** Contact support any day of the week.

Protect your email traffic – without investing in hardware and software

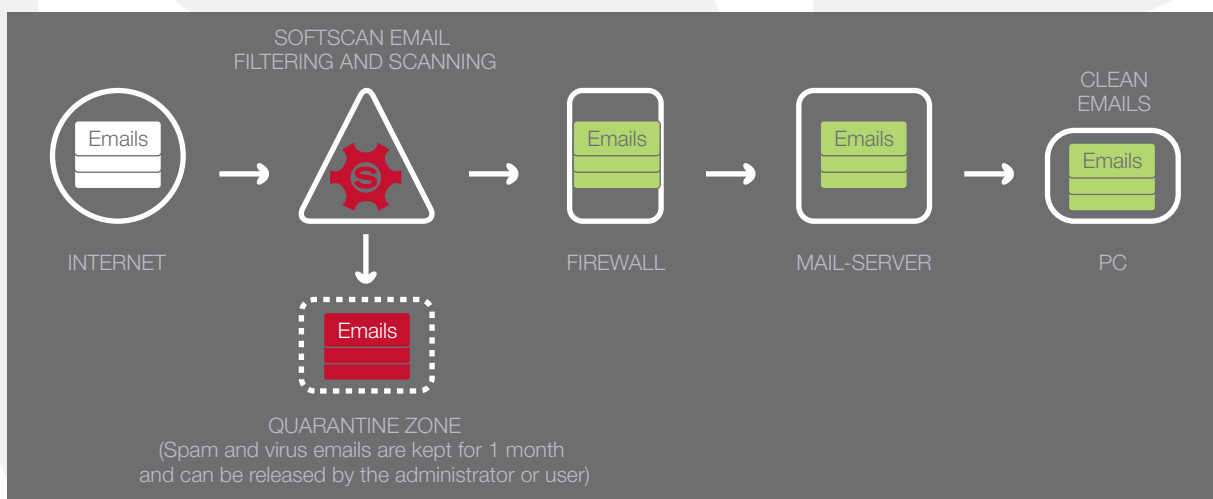
SoftScan protects your email communications with market leading spam and virus scanners combined with SoftScan's own intelligent scanner, Paranoid.

SoftScan is a hosted service, which means that your organisation is completely free from managing installations or software updates – the solution is constantly updated and optimised by knowledge gained from the millions of emails that are scanned everyday by SoftScan.

Everything is done for you – you simply route your email traffic through SoftScan. All emails pass through SoftScan's security service. Infected and unwanted emails are sent to the quarantine zone and only clean email is delivered to your own mail server (with an imperceptible delay).

In addition, you can choose to send all outgoing emails via SoftScan, which will ensure that no viruses are sent from your organisation.

How the SoftScan email security service works



SoftScan manages your email traffic through several spam and virus filters that scan emails against thousands of rules. Once the email has been scanned for unwanted and harmful content, approved emails are then sent to your mail server.

The components of SoftScan email security service

The strength behind SoftScan's service lies in its ability to combine a number of components together to provide maximum security.

Reputation Filter

The first defence in SoftScan's service is the Reputation Filter, which automatically blocks emails from servers that are known to deliver spam. In this way, large quantities of spam can be removed, reducing the load on the scanning system and minimising the effects of new techniques introduced by spammers.

When an email is accepted by SoftScan's servers, the Reputation Filter performs an assessment of the sender. It looks-up the IP address in a number of internal and external databases that collect data about the senders of spam and viruses.

SoftScan constantly monitors and rates the quality of the external databases to ensure that it only blocks emails from "black-listed" senders.

When an email is rejected by the Reputation Filter the sender will immediately receive a status email explaining the reason for the rejection.



Spam filter

SoftScan detects spam using a combination of several techniques including signature matches with other known spam messages, content analysis, the use of black and white lists, including messages that have links to blacklisted URLs. Also Bayesian filtering, whereby statistics determine the likelihood of different words appearing in spam or non spam messages is part of the spam filtering process. In addition, SoftScan's spam filter supports the Sender Policy Framework and can protect you against receiving large numbers of delivery reports when your domain has been spoofed to send spam messages, known as Joe-Jobs.

The Optical Character Recognition filter used by SoftScan is also able to detect the sophisticated use of image spam by recognising messages, even when the sender has obfuscated the text within a picture file.

Scanners are updated automatically every 15 minutes, and all anti-spam scanning can be configured to your own tolerance levels.

Three leading virus scanners

The solution uses three leading virus scanners ClamAV, Kaspersky and Trend Micro. The three conventional anti-virus scanners work together with SoftScan's own heuristic scanner Paranoid to protect against unwanted emails.

Paranoid

Paranoid constantly analyses patterns in the emails it accepts to ensure that it stops as yet unknown viruses, before traditional antivirus scanners have updated their filters.

Paranoid learns and updates with every email it scans. The result is a scanner that is extremely effective with almost no false positives.

Paranoid provides an additional layer of configurable scanning features that are able to detect suspicious content or block emails which violate an organisation's security policy. A particular function of Paranoid is Virus Probability Analysis (VPA). The VPA scans and analyses all emails as they pass through the system, identifying and categorising viruses, that are not yet known by conventional anti-virus scanners.

User configuration

Do you want the sales department to be protected against spam? Or would they prefer prompt notification of any email stopped? Should marketing be the only department that can receive large files? Do you require a copy of every email to be backed-up?

SoftScan's web based administrators console allows you to navigate and set-up the solution to reflect your own email policy, personal preferences or local legislation. Eg. you can set up the system to filter mails from specific senders and domains.

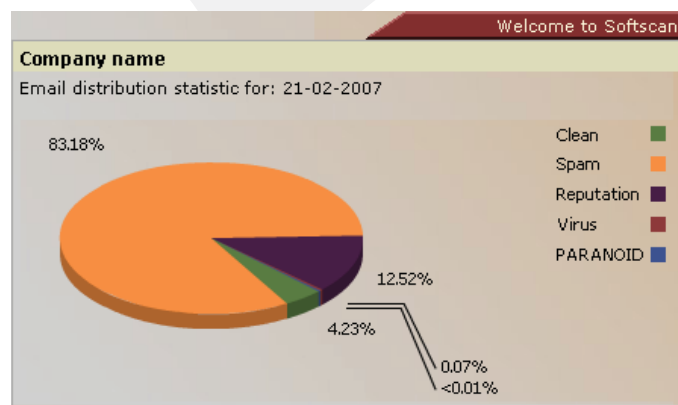
If you require additional security, the system can be configured to remove all content that may be harmful within your emails, and only allow the content text. This feature is a benefit to users of mobile phones and PDAs, which have low bandwidth capabilities.

Features and functions

Overview

The administrators' console provides a complete overview as you login. The opening screen provides you with all of the main information:

- Today's statistics of email distribution by the categories: clean, virus, spam and paranoid.
- Potential false positives (emails that have incorrectly been identified as spam) since last login or in the last 24 hours.
- Outgoing emails from your server, which were infected by a virus.
- Emails that are queued, waiting to be delivered.



Secure Storage of emails

If your own email server is down, you don't need to worry about lost emails because the system is able to place your emails in a queue. Once the problem is resolved, SoftScan sends you all the emails that have accumulated during this time.

All emails are kept for 7 days and a status email about unsuccessful delivery is sent to the sender.

Encrypted emails

The system can also be configured to send-on messages that use a digital signature or are encrypted – which is useful if you have a server that handles emails with digital signatures.

SoftScan's system supports point-to-point encryption from SMTP communications using "Transport Layer Security" (TLS). TLS is the protocol that is supported by most email servers and ensures that nobody can obtain unauthorised access to email or monitor the SMTP traffic between sender and recipient.

LDAP

SoftScan's Advanced Recipient Handling function makes it possible for to integrate the SoftScan system with the organisation's LDAP server (eg: Microsoft Active Directory, Lotus Domino) and configure how the system should react to emails sent to invalid mail address. Eg. you can determine whether or not SoftScan should stop all emails to invalid recipients.

Intelligent Quarantine Service [IQS]

You can activate the Intelligent Quarantine Service (IQS) to handle all messages that have been placed in quarantine. Every email account will receive a daily report, which displays the most likely false positives, any messages that should not be quarantined can easily be released and the message is delivered immediately.

Datacentre

To guarantee the security of the system, SoftScan has several datacentres placed at various physical locations. Datacentres are managed and monitored by experts in the security field and are safeguarded at multiple levels to protect against unauthorised access.

Support

If you have a question, SoftScan's support team is available by phone and email every day of the week between 8.30-22.00 CET.

About SoftScan

SoftScan is Scandinavia's leading provider of antivirus and spam filtering solutions. SoftScan was established in 2003, and has over 100 employees. The solution is sold in Denmark, Sweden, Norway, United Kingdom, Eire and Germany, and is used in over 100 countries.

Every day over 90 million emails flow through SoftScan's scanning system. On average 90-95% of emails scanned are spam, and less than 1% contain viruses.



SoftScan
+44 (0)20 7956 2029
www.softscan.co.uk