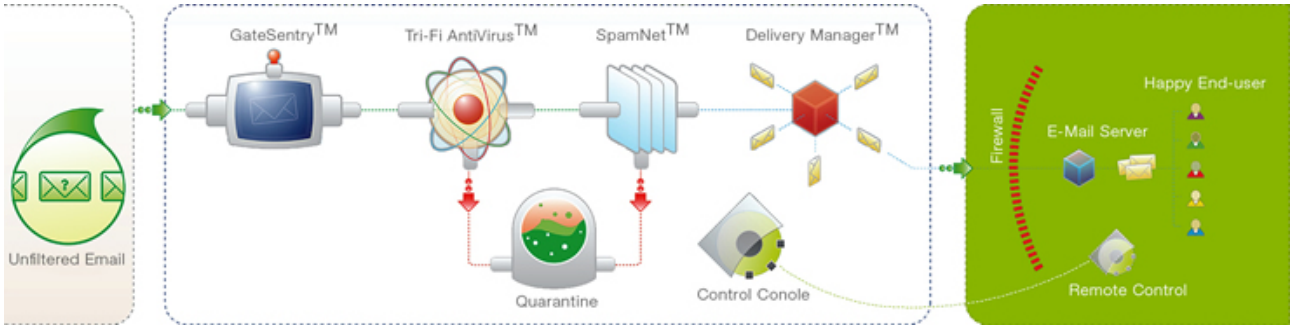
# Antispam & Antivirus

## Factsheet

| | M | L |
|---|---|---|
| **Features** | | |
| **Inbox protection** | Yes | Yes |
| **Outbox protection** | - | Yes |
| **Number of e-mail accounts** | 5 – 5‘000 | 5 – 5‘000 |
| **Billing** | | |
| **Subscription period** | 12, 24, 36 months | 12, 24, 36 months |
| **Billing period** | 3 months | 3 months |
| **One-time setup fee** | CHF 270.– | CHF 270.– |

## Everything you need to know:




**GateSentry:**
Access to SpamLab is subject to maximum security monitoring so that our SpamLab cannot be blocked by attacks or hackers. Only the best equipment is used and all equipment is redundant.

**Tri-Fi AntiVirus:**
The three virus scanners (McAfee, SOPHOS and FPROT) remove viruses, trojans, worms, and other dangerous contents from your e-mails. The virus scanner is updated in real time every 10 minutes.

**SpamNet:**
SpamNet scans each e-mail for various spam characteristics. Our current spam identification functionality can be described as follows:

- Header, Subject, Lexical, Signatures Analyse
- Multi-hop detections
- URL screening
- Heuristic-Methodic
- Image decoding and detection
- Anti-spoofing
- HTML Tag Parsing
- Campaingn tracking analysis
- Internal and External block Lists

**Delivery Manager:**
The delivery manager architecture increases the stability and availability of SpamLab. Only “real” e-mails are delivered to the customer server.

**Quarantine:**
All suspicious e-mails land in quarantine so that no e-mail is unintentionally lost.

**Web interface (Control Console):**
The web interface serves as login. All e-mails in quarantine can be viewed without downloading dangerous contents. Additionally, all settings and details can be viewed and changed by the customer.

## How the antispam solution works

**Analysis of the subject line:**
Many spam e-mails have recognizable, known subject lines that can be used to filter our newly sent spam e-mails.

**Anti-relay function:**
Protects the mail server so that it cannot be used as a spammer. This prevents being listed in real-time blacklists.

**Antispam database:**
Databases on the Internet that contain examples of known spam e-mails. Mail servers can compare e-mails with these databases and block e-mails found in the databases.

**Anti-spoofing:**
Recognizing spammers whose e-mails are actually from external domains, but are camouflaged with internal sender addresses.

**Header analysis:**
Analyzing the e-mail header to determine discrepancies from defined e-mail standards.

**Heuristic analysis:**
Rule-based scan methods that recognize specific e-mail characteristics. Characteristics like “Removelink” and certain words like “VIAGRA” indicate spam and are assigned “bad points”. Following the analysis, the points are added. If they exceed a defined threshold, an e-mail is classified as spam.

**Internal blacklists and whitelists:**
Lists with domain names and addresses that are explicitly blocked. Whitelists are the counterpart, clearly specified as wanted e-mails.

**Lexical text analysis:**
Examination of entire sections of text and links using operators like OR, AND, NOT, etc. to find, for example, sales pitches and requests to visit websites.

**Real-time blacklists (RBL):**
Lists on the Internet containing IP addresses of mail servers that have sent spam. RBLs prevent company servers from accepting e-mails from such known IP addresses. It is possible that mail servers are incorrectly placed on these lists when company servers were unwillingly forced to send spam.

**Protection against mail bombing:**
Preventing a mail server from sending a massive amount of automatically generated e-mails (DoS, denial of service). This protection regulates e-mail traffic to prevent overloading.

**Preventing directory harvesting attacks:**
Stop attempts by spammers to find valid e-mail addresses via the SMTP server.

## Solution advantages

- Easy installation by rerouting mail traffic (MX record)
- No own antispam/antivirus infrastructure necessary
- Antispam analyzes and sorts your e-mails
- No more annoying sorting of unwanted e-mails
- Spam, viruses and trojans remain in our quarantine
- Improved productivity and more security
- Own infrastructure protected from malicious e-mails
- No unnecessary loading of your infrastructure due to unnecessary data traffic